PANOWANIE NAD RYZYKIEM W RAMACH PUBLICZNEGO ZARZĄDZANIA KRYZYSOWEGO

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Witold Skomra

PANOWANIE NAD RYZYKIEM W RAMACH PUBLICZNEGO ZARZĄDZANIA KRYZYSOWEGO

WARSZAWA 2018

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Recenzenci:
Prof. dr hab. inż. Jacek Szołtysek (Uniwersytet Ekonomiczny w Katowicach)
Prof. dr hab. Krzysztof Malik (Politechnika Opolska)

Projekt okładki:
Agnieszka Kownacka

Korekta:
Anna Pacek

© Copyright by Witold Skomra, Warszawa 2018
© Copyright by BEL Studio Sp. z o.o., Warszawa 2018

Wydanie pierwsze, elektroniczne, Warszawa 2018

Realizacja wydawnicza: *BEL Studio Sp. z o.o.*
01-355 Warszawa
ul. Powstańców Śl. 67 B
tel./fax (+48 22) 665 92 22
e-mail: studio@bel.com.pl
www.bel.com.pl
księgarnia: http://www.iknt.edu.pl

ISBN: 978-83-7798-358-4

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Spis treści

Wykaz najważniejszych skrótów 7
Wprowadzenie 9

Rozdział I
Elementy zarządzania kryzysowego w administracji publicznej 27
1.1. Proces kształtowania zarządzania kryzysowego w polskim systemie prawnym 27
1.2. Zakres zadań realizowanych w ramach zarządzania kryzysowego 30
1.3. Fazy zarządzania kryzysowego 32
1.3.1. Faza pierwsza – zapobieganie 34
1.3.2. Faza druga – przygotowanie 35
1.3.3. Faza trzecia – reagowanie 36
1.3.4. Faza czwarta – odbudowa 36
1.4. Kierowanie i koordynacja działań w ramach zarządzania kryzysowego . . 37
1.4.1. Szczebel centralny 37
1.4.2. Szczebel wojewódzki 39
1.4.3. Szczebel samorządowy 40
1.5. Struktura organizacyjna zarządzania kryzysowego 44
1.5.1. Szczebel centralny 44
1.5.2. Szczebel wojewódzki 47
1.5.3. Szczebel samorządowy 49
1.6. Współdziałanie organów zarządzania kryzysowego 50
1.7. Planowanie w zarządzaniu kryzysowym 53
1.7.1. Cykl planowania 53
1.7.2. Raport o zagrożeniach bezpieczeństwa narodowego 55
1.7.3. Siatka bezpieczeństwa 70
1.8. Podsumowanie rozdziału 82

Rozdział II
Ochrona infrastruktury krytycznej 83
2.1. Pojęcie infrastruktury krytycznej 83
2.2. Proces wyłaniania IK przy podejściu systemowo-obiektowym 85
2.3. Zarządzanie ryzykiem w ochronie IK 86
2.4. Podsumowanie rozdziału 90

Rozdział III
System zarządzania kryzysowego w ujęciu teoretycznym 91

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

3.1. Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego 91
3.2. Zarządzanie społecznymi skutkami zmaterializowania się ryzyka 96
3.3. Zarządzanie kryzysowe w naukach o bezpieczeństwie i w naukach o zarządzaniu 99
3.4. Podsumowanie rozdziału 103

Rozdział IV
Zarządzanie ryzykiem w administracji publicznej 105

4.1. Formy postępowania z ryzykiem w administracji publicznej 105
4.2. System zarządzania kryzysowego jako element organizacji państwa . . . 109
4.3. Ujęcie procesowe w zarządzaniu ryzykiem 110
4.4. Cele systemu zarządzania kryzysowego 115
4.5. Podsumowanie rozdziału 118

Rozdział V
Elementy zarządzania ryzykiem w publicznym zarządzaniu kryzysowym . . . 119

5.1. Ryzyko operacyjne w zarządzaniu kryzysowym 119
5.2. Zarządzanie reputacją i komunikacją kryzysową 129
5.3. Zintegrowane zarządzanie ryzykiem w ramach zarządzania kryzysowego 132
5.4. Elementy ekonomiki w zarządzaniu ryzykiem i niepewnością 139
5.5. Podsumowanie rozdziału 145

Rozdział VI
Zarządzanie ryzykiem wystąpienia sytuacji kryzysowej 147

6.1. Zarządzanie podatnością 147
6.2. Budowanie barier systemowych i suplementowych 152
6.3. Źródła sytuacji kryzysowych 155
6.3.1. Ciągłość działania 156
6.3.2. Zarządzanie ryzykiem bezwarunkowym i warunkowym 158
6.3.3. Zagrożenia wewnątrzsystemowe 159
6.3.4. Zdarzenia nieprzewidywalne 160
6.4. Podsumowanie rozdziału 162

Zakończenie 163
Załącznik – Raport z badań 169
Bibliografia 177
Akty prawne i normatywne 187
Orzecznictwo 193
Strony internetowe 193
Spis rysunków, schematów i tabel 195

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Wykaz najważniejszych skrótów

Akty prawne

kk – Ustawa z dnia 6 czerwca 1997 r. Kodeks karny [DzU nr 88, poz. 553 ze zm.]

Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. [DzU nr 78, poz. 483 ze zm.]

kpa – Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego [tekst jedn. DzU z 2016 r. poz. 23]

nowelizacja UZK – Ustawa z 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym [DzU nr 131, poz. 1076]

RoZBN/raport – Raport o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy o zarządzaniu kryzysowym i w rozporządzeniu Rady Ministrów z 30 kwietnia 2010 r. [DzU nr 83, poz. 540]

UMOL/decyzja – decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności [DzUrz UE L 347/924]

UZK/ustawa – Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym [tekst jedn. DzU z 2017 r. poz. 209]

Inne

ABW – Agencja Bezpieczeństwa Wewnętrznego

AW – Agencja Wywiadu

CAT ABW– Centrum Antyterrorystyczne ABW

EPOIK – Europejski Program Ochrony Infrastruktury Krytycznej

GIIF – Generalny Inspektor Informacji Finansowej

GIOŚ – Główny Inspektorat Ochrony Środowiska

IK – infrastruktura krytyczna

IMGW – Instytut Meteorologii i Gospodarki Wodnej

KE – Komisja Europejska

KGP – Komenda Główna Policji

KGPSP – Komenda Główna Państwowej Straży Pożarnej

KPKZ – Krajowy Plan Zarządzania Kryzysowego

KZGW – Krajowy Zarząd Gospodarki Wodnej

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

MRiRW – Ministerstwo Rolnictwa i Rozwoju Wsi
MSWiA – Ministerstwo Spraw Wewnętrznych i Administracji
MŚ – Ministerstwo Środowiska
MZ – Ministerstwo Zdrowia
NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej
OECD – Organizacja Współpracy Gospodarczej i Rozwoju
PAA – Państwowa Agencja Atomistyki
PSP – Państwowa Straż Pożarna
RCB – Rządowe Centrum Bezpieczeństwa
RM – Rada Ministrów
RZZK – Rządowy Zespół Zarządzania Kryzysowego
WCZK – Wojewódzkie Centrum Zarządzania Kryzysowego
WZZK – Wojewódzki Zespół Zarządzania Kryzysowego

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Wprowadzenie

Zapewnienie bezpieczeństwa jest od zawsze podstawowym zadaniem państwa. Bezpieczeństwo pojmowane tradycyjnie jako stan braku zagrożenia z czasem zaczęło być postrzegane jako proces. W tym sensie bezpieczeństwo danego podmiotu to ta dziedzina jego aktywności, której treścią jest zapewnianie możliwości przetrwania (egzystencji) i swobody realizacji własnych interesów w niebezpiecznym środowisku, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), stawianie czoła wyzwaniom, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów (Koziej 2010). W celu zapewnienia bezpieczeństwa budowano i nadal buduje się struktury zdolne do reakcji na wypadek wystąpienia zakłócenia. Jednak z czasem zaczęto zwracać uwagę na działania prewencyjne, których celem powinno być zapobieganie tym zagrożeniom, które jeszcze nie wystąpiły (lub występowały w przeszłości), a których pojawienie się jest prawdopodobne. Jednym z narzędzi do całościowego podejścia do zagrożeń jest zarządzanie kryzysowe. Potrzeba powołania nowej struktury zdolnej do całościowego zarządzania problematyką zdarzeń i katastrof w przypadku Polski wynikała z negatywnych doświadczeń po powodzi z 1997 r. Uznano wówczas, że dotychczasowe struktury powołane do działania w takich sytuacjach są niewydolne. Zarządzanie kryzysowe, choć ukierunkowane na reakcję po wystąpieniu zagrożenia, od początku stosowało ocenę ryzyka i elementy zarządzania ryzykiem w celu racjonalizacji wysiłków i nakładów finansowych na poszczególne rodzaje zagrożeń. Jednocześnie stale doskonalono wszystkie elementy struktury organizacyjnej poprzez procesy planowania i testowania. Przełomem w dalszym rozwoju zarządzania kryzysowego jest wejście w życie Unijnego Mechanizm Ochrony Ludności (DzUrz UE L 347/924, dalej UMOL). Ta decyzja postawiła przed administracją wszystkich krajów UE zupełnie nowe wyzwanie. Państwa członkowskie mają obowiązek zarządzania ryzykiem. Oznacza to odejście od zarządzania bezpieczeństwem w sposób reaktywny (jako odpowiedź na zdarzenie, które już nastąpiło) i skoncentrowanie się na procesie całościowym, gdzie zapobieganie zagrożeniom (a ściślej różnym rodzajom ryzyka, jakie te zagrożenia ze sobą niosą) jest równie ważne jak reakcja po zmaterializowaniu się ryzyka. Równocześnie niezbędnym jest zbudowanie i stałe utrzymywanie odpowiedniego poziomu gotowości rozumianego jako adekwatny do wielkości ryzyka stan zasobów ludzkich, technicznych i organizacyjnych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Praca jest podsumowaniem wieloletnich obserwacji i badań autora nad zagadnieniem zagrożeń i różnych rodzajów ryzyka, z jakimi administracja publiczna musi się zmierzyć, budowania struktur zdolnych do zarządzania w sytuacji wystąpienia zagrożenia, procesów kierowania, współdziałania i koordynacji oraz czynników, które wpływają na sprawność tych procesów. Zagadnienia te pojawiały się we wcześniejszych opracowaniach autora. Koncentrowały się one na czterech obszarach:

1. W zakresie kierowania, współdziałania i koordynacji[1].
2. W zakresie budowania struktur zarządzania kryzysowego[2].
3. W zakresie zarządzania kryzysowego[3].

[1] *Problemy organizacyjno-prawne współdziałania administracji, wojska i służb ratowniczych w czasie klęski żywiołowej*, „Zeszyty Naukowe Akademii Obrony Narodowej", nr 1/2004.

Podział kompetencji pomiędzy organami administracji publicznej podczas zwalczania katastrof i klęsk żywiołowych, [w:] *Samorząd a ochrona środowiska*, praca zespołowa pod redakcją Marii Suchy i Jana Trzebińskiego, Biblioteka Monitoringu Środowiska, Wojewódzki Inspektorat Ochrony Środowiska, Rzeszów 2006.

Funkcjonowanie organów administracji publicznej w czasie klęsk żywiołowych w wybranych krajach, „Bezpieczeństwo i Technika Pożarnicza", kwartalnik CNBOP, nr 1/2007.

Praktyczne aspekty współdziałania administracji centralnej i terenowej oraz rządowej i samorządowej przy tworzeniu systemu bezpieczeństwa cywilnego, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, dydaktyki i praktyki*, praca zbiorowa pod redakcją Bogdana Kosowskiego i Andrzeja Włodarskiego, Warszawa 2007.

Współdziałanie służb i administracji w sytuacjach kryzysowych na obszarach przygranicznych, [w:] *Zadania Policji i innych służb na tle potrzeb społecznych*, praca zbiorowa pod red. Władysława Tabasza i Jacka Strojnego. „Biblioteka Ropczycka", zeszyt nr 10, wrzesień 2008.

Strategiczne warunki bezpieczeństwa narodowego RP; prognostyczne scenariusze w perspektywie 20 lat, opracowanie zespołowe (ekspertyza). Współautorzy: dr Andrzej Towpik, dr Jerzy Nowak, dr Edward Kirejczyk, prof. dr hab. Stanisław Parzymes, prof. dr hab. Marek Pietras, mgr Adam Balcer. Materiał niejawny dostępny w Biurze Bezpieczeństwa Narodowego.

[2] *Struktura zarządzania kryzysowego w państwie – logika systemu*, [w:] *Bezpieczeństwo i zarządzanie kryzysowe – aktualne wyzwania. Perspektywy rozwoju teorii i badań nad zarządzaniem bezpieczeństwem*, (red.) M. Włodarczyk, A. Marjański, tom X, zeszyt 5, SWSPiZ, Łódź 2009.

Rola organów zarządzania kryzysowego w sytuacjach nadzwyczajnych i kryzysowych, [w:] *Zarządzanie kryzysowe w administracji publicznej*, (red.) J. Kisielnicki, A. Letkiewicz, K. Rajchel, E. Ura, Warszawa 2010.

Warianty działania administracji publicznej w sytuacji kryzysowej, [w:] „Problemy ochrony granic", biuletyn Centrum Szkolenia Straży Granicznej, nr 46/2010, Kędzierzyn 2010.

Współpraca administracji z sektorem gospodarczym na rzecz ochrony infrastruktury krytycznej, „Management Science Review", 1(1) 2017 UE Wrocław (rozwinięciem tego artykułu jest treść rozdziału II).

Miejsce, rola i zadania Rządowego Centrum Bezpieczeństwa w zakresie integracji działań na rzecz utrzymania bezpieczeństwa, [w:] *Ratownictwo wodne oraz inne aspekty bezpieczeństwa na obszarach wodnych*, (red.) J. Telak, CSP, Legionowo 2017.

[3] *Ochrona Infrastruktury Krytycznej w Systemie Zarządzania Kryzysowego*, [w:] *Ochrona infrastruktury krytycznej*, praca zbiorowa pod red. A. Tyburskiej, Wydawnictwo WSpol., Szczytno 2010.

Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy, Wyd. Presscom, Wrocław 2010.

Zarządzanie kryzysowe – praktyczny przewodnik, Wyd. Presscom, Wrocław 2016, (na bazie tej monografii opracowano rozdział I i częściowo rozdział II).

Ekspertyza *Kierunki doskonalenia zarządzania kryzysowego w ramach systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa*,W. Skomra, M. Wągrowska, RCB, styczeń 2017 (materiał niepublikowany).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

4. W zakresie zarządzanie ryzykiem[4].

Wymienione prace wskazują na trzy powiązane ze sobą obszary problemowe:

1. System zarządzania kryzysowego, pomimo poprawnie zorganizowanej struktury, zależności wewnątrzsystemowych oraz zadań, wielokrotnie zawodził w konfrontacji z realnymi zagrożeniami. Fakt ten wskazuje na konieczność zbadania przyczyn tego zjawiska i wskazania środków zaradczych.
2. Wdrożenie zarządzania ryzykiem jako jednego z zasadniczych celów działania administracji publicznej wymaga odpowiedniej podbudowy naukowej.
3. Wymienione obszary problemowe można połączyć w szersze zagadnienie o charakterze teoriotwórczym. Nauki o bezpieczeństwie pomijają zagadnienie postępowania z ryzykiem. Natomiast nauki o zarządzaniu rozwijają zagadnienie identyfikowania, oceny i postępowania z ryzykiem, nie odnoszą ich jednak do administracji publicznej i struktur przez nią powoływanych.

Rozważania prowadzone ramach niniejszego opracowania koncentrowały się na tych trzech zasadniczych zagadnieniach. Jednocześnie już w tytule wskazano na jeden z problemów związanych z pojęciami stosowanymi w literaturze. W opracowaniach anglojęzycznych postępowanie z ryzykiem określane jest terminem „risk management". Pojęcie to zostało przetłumaczone jako „zarządzanie ryzykiem" i pod tą nazwą występuje w literaturze krajowej. W rzeczywistości jest to tłumaczenie błędne, a przynajmniej nie oddające istoty zagadnienia (Turski 2013). Słowo „managament" wiąże się z czasownikiem „to manage", który oznacza: „kierować, radzić sobie, dawać sobie radę z czymś" (internetowy słownik Diki). Natomiast „zarządzanie" to nic innego jak „sprawowanie zarządu" (internetowy słownik języka polskiego PWN), czyli działalność związana ze sprawowaniem władzy. Zasadniczym celem postępowania z różnymi rodzajami ryzyka nie jest sprawowanie nad nimi władzy, lecz „keep risks under control" (Carretta, Fiordelisi, Schwizer 2017), co odpowiada określeniom „radzenie sobie z nimi", „zapanowanie nad nimi". W niniejszym opracowaniu będzie wprawdzie stosowane określenie „zarządzanie ryzykiem", ze względu na jego powszechność w literaturze, ale należy pamiętać o jego prawidłowym rozumieniu. W efekcie w ramach zarządzania kryzysowego (definicja zostanie przytoczona w dalszej części), będziemy mieć do czynienia jednocześnie z działaniem planowym w odniesieniu do

[4] *Zdolność zarządzania ryzykiem jako nowe wyzwanie dla system zarządzania kryzysowego*, [w:] *Zarządzanie kryzysowe w wymiarze lokalnym, organizacja, procedury, organy i instytucje*, praca zbiorowa pod redakcją D. Majchrzak, AON, 2014 r.

Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego Rzeczypospolitej Polskiej, [w:] „Prace i studia geograficzne", tom 55, praca zbiorowa, red. E. Smolska, M.W. Solarz, U. Somorowska, M. Tomczuk, Wydział Geografii i Studiów Regionalnych UW, 2014.

Zarządzanie ryzykiem. Przegląd wybranych metodyk, praca zbiorowa, red. D. Wróblewski, CNBOP, Józefów 2015.

Risk management as part of crisis management tasks, „Foundations of Management", vol. 9, (2017), pp. 245–256 (artykuł został wykorzystany przy opracowywaniu rozdziału V).

Zarządzanie ryzykiem operacyjnym w administracji publicznej, „Przegląd Organizacji", nr 7/2017 (artykuł został wykorzystany przy opracowywaniu rozdziału VI).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

przewidywalnych przyszłych zdarzeń oraz z przygotowaniem się na przejęcie kontroli („zapanowanie") nad przyszłą sytuacją, której w danym momencie przewidzieć się nie da. Tak rozszerzone zarządzanie ryzykiem jest realizowane w obszarze publicznym, gdzie określenie „publiczny" oznacza „dostępny lub przeznaczony dla wszystkich" (internetowy słownik języka polskiego PWN). Podmiotami sprawującymi to zarządzanie są zarówno organy administracji, jednostki organizacyjne sektora finansów publicznych, jak i podmioty gospodarcze, które na mocy prawa zostały zobowiązane do zarządzania ryzykiem.

Cel i główny problem badawczy

Wprowadzenie zarządzania ryzykiem jako głównego zadania dla systemu zarządzania kryzysowego oraz podejścia procesowego do opisu działań realizowanych przez ten system stawia problem podbudowy naukowej dla tak rozumianego zarządzania. Do niedawna taką podbudową były osiągnięcia nauk o bezpieczeństwie. Jednak po zmianie podejścia co do roli zarządzania kryzysowego w administracji publicznej[5] pojawiają się elementy wspólne z badaniami prowadzonymi na gruncie nauk o zarządzaniu. Dotyczą one zarówno zagrożeń i skutków, jakie mogą dotknąć samą organizację, jak i celów, które organizacja chce osiągnąć. Z tego punktu widzenia wymagany postanowieniami UMOL proces postępowania z ryzykiem (szczegóły tego procesu zostaną przedstawione w rozdziale 5), w odniesieniu do budowania gotowości, wykazuje analogię z zarządzaniem ryzykiem stosowanym w biznesie. Identyfikujemy zagrożenia, oceniamy i szacujemy ryzyko, a na tej podstawie podejmujemy decyzje co do metody zarządzania nim (Zawiła-Niedźwiecki 2013). Zastosowanie podejścia procesowego do opisu działań zarządzania kryzysowego pozwala przeanalizować zagadnienie zarządzania ryzykiem operacyjnym, które jest charakterystyczne dla każdej organizacji. Istnieją jednak znaczące różnice pomiędzy celami, dla których stosuje się zarządzanie ryzykiem. O ile dla zarządzania kryzysowego jest to ochrona ludzi, ich zdrowia, mienia oraz środowiska, to dla zarządzania ryzykiem operacyjnym jest to utrzymanie celów działania organizacji (Ronka-Chmielowiec 2010).

Na bazie tego spostrzeżenia został sformułowany cel niniejszego opracowania, którym jest uogólnienie teoretyczne działań administracji publicznej podejmowanych wobec zagrożeń. Zakres badań teoriotwórczych obejmuje:

- powiązanie zarządzania bezpieczeństwem narodowym z zarządzaniem ryzykiem bezwarunkowym i warunkowym realizowanym w ramach zarządzania kryzysowego;
- powiązanie podejścia systemowego i procesowego w celu właściwego opisu działań w obszarze zarządzania kryzysowego;
- poszerzenie pojęcia „organizacja" na struktury tworzone przez administrację publiczną w celu zarządzania sytuacją kryzysową, w tym również struktury powoływane doraźnie;

[5] Zmiana ta polega na wprowadzeniu obowiązku zarządzania ryzykiem i jest wynikiem wejścia w życie znowelizowanego Unijnego Mechanizmu Ochrony Ludności. Zagadnienie to zostanie omówione w dalszej części.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

– uwzględnienie zarządzania ryzykiem operacyjnym jako jednego z elementów towarzyszących zarządzaniu ryzykiem bezwarunkowym i warunkowym.

Aby osiągnąć powyższy cel należy w pierwszej kolejności udzielić odpowiedzi na pytanie będące głównym problemem badawczym:

Jakie zależności występują pomiędzy ryzykiem operacyjnym a pozostałymi ryzykami, którymi zarządza się w ramach publicznego zarządzania kryzysowego?

Pytaniu temu towarzyszyło pytanie pomocnicze:

Przy jakich uwarunkowaniach struktury powoływane doraźnie w ramach administracji publicznej można uznać za organizacje?

Efekty prac teoriotwórczych związanych z tak określonym celem przedstawiono w zakończeniu.

Podstawowe pojęcia i definicje

Podstawowym pojęciem wokół którego koncentrowały się badania jest „ryzyko operacyjne", który to termin wiąże się z pojęciami „operacja" oraz „operacyjny". Przez operację należy rozumieć „działania zmierzające do wykonania określonego zadania" (*Słownik języka polskiego PWN*). Poszczególne operacje układają się w procesy. Proces to zbiór czynności wymagający na wejściu wkładu i dający na wyjściu rezultat mający pewną wartość dla klienta (Gabryelczyk 2006). Proces wiąże się z działaniem stałym, ciągłym, rutynowym, będącym często zadaniem interdyscyplinarnym w stosunku do organizacji przedsiębiorstwa (Niedbała, Sierpińska 2003). Zarządzanie operacyjne zajmuje się sposobem wykonywania operacji i jest związane z podejściem procesowym. Według tego podejścia działalność organizacji odbywa się w formie procesów polegających na realizacji kolejnych operacji (Waters 2001).

Dla celów procesu badawczego przyjęto następujące znaczenie poszczególnych pojęć:

- działanie – dowolne zachowanie się, zmierzające do osiągnięcia celu, polegające na wykonaniu czegoś lub powstrzymaniu się od czegoś (Zieleniewski 1975, s. 165);
- funkcjonowanie – zachowanie się grupy wiążące się z określonym działaniem jej członków (Zieleniewski 1975, s. 166);
- zarządzanie - działalność kierownicza polegająca na ustalaniu celów i powodowaniu ich realizacji (*Encyklopedia organizacji i zarządzania*, 1981, s. 609);
- zagrożenie statyczne – niekorzystne zjawisko, które nie ulega istotnym zmianom lub jest niezmienne w określonym czasie;
- zagrożenie dynamiczne – niekorzystne zjawisko, które jest efektem szybkich zmian zachodzących w organizacji i jej otoczeniu;
- zdarzenie krytyczne – zdarzenie, które warunkuje dalszy ciąg zdarzeń;
- ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niekorzystnego i jego skutków (ewentualnie podatności i spodziewanych skutków);
- ryzyko odłożone – ryzyko, które wynika z działalności człowieka, a negatywne skutki tego oddziaływania na ludzi, otoczenie cywilizacyjne i środowisko naturalne są odłożone w czasie;

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

- ryzyko bezwarunkowe – ryzyko, którego występowanie nie jest uzależnione od wystąpienia zdarzenia krytycznego;
- ryzyko warunkowe – ryzyko, którego występowanie jest uzależnione od wystąpienia zdarzenia krytycznego;
- podatność – cecha organizacji determinowana przez jej słabe punkty lub luki w zabezpieczeniach określająca stopień, w jakim oddziaływanie na nią różnych rodzajów ryzyka może prowadzić do niepożądanych zdarzeń;
- odporność – zdolność systemu, społeczności narażonej na zagrożenia do odparcia, wchłonięcia, przystosowania i odbudowy związanej ze skutkami zagrożenia dokonanej w odpowiednim czasie i w skuteczny sposób, włączając w to utrzymanie i odtworzenie ich podstawowych struktur i funkcji (*Risk Assessment and Mapping Guidelines for Disaster Management*, 2010);
- zarządzanie ryzykiem – identyfikowanie potencjalnych zdarzeń bądź sytuacji, szacowanie ich skutków oraz prawdopodobieństwa wystąpienia, określenie i zastosowanie odpowiednich sposobów reagowania, a także monitorowanie ryzyka (Korombel 2013, s. 43);
- sytuacja kryzysowa – sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków (DzU z 2017 r. poz. 209, art. 3 pkt. 1);
- zarządzanie sytuacją kryzysową – proces polegający na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej (DzU z 2017 r. poz. 209, art. 2);
- ryzyko wystąpienia sytuacji kryzysowej – kombinacja prawdopodobieństwa wystąpienia zdarzenia niekorzystnego oraz zawodności barier suplementowych i systemowych, gdzie bariery suplementowe to bariery ograniczające lub zwiększające skutki zagrożeń, wynikające z wrażliwości i odporności danej społeczności, zaś bariery systemowe to bariery ograniczające skutki zagrożeń, tworzące system ochrony społeczności przed zagrożeniami (Skomra 2015, s. 192–204);
- zarządzanie kryzysowe – działalność organów administracji publicznej będąca elementem utrzymania bezpieczeństwa narodowego, która polega na:
  - identyfikowaniu zagrożeń,
  - zarządzaniu ryzykiem,
  - zarządzaniu sytuacją kryzysową, w tym spowodowaną dysfunkcją infrastruktury krytycznej (definicja własna),
- ryzyko operacyjne (w publicznym zarządzaniu kryzysowym) – jest to ryzyko negatywnego oddziaływania na życie i zdrowie ludzi, mienie (w tym dziedzictwo kulturowe), środowisko naturalne, gospodarkę i infrastrukturę krytyczną oraz ryzyko strat materialnych i reputacyjnych, wynikających

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku procesu zmian w środowisku naturalnym, polityczno-militarnym i społeczno-kulturowym oraz w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych (opracowanie własne);

- ryzyko operacyjne (w zarządzaniu sytuacją kryzysową) – jest to ryzyko strat materialnych i reputacyjnych oraz odpowiedzialności prawnej, wynikających z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych (Zawiła-Niedźwiecki 2013, s. 62).

Założenia podlegające weryfikacji w procesie badawczym

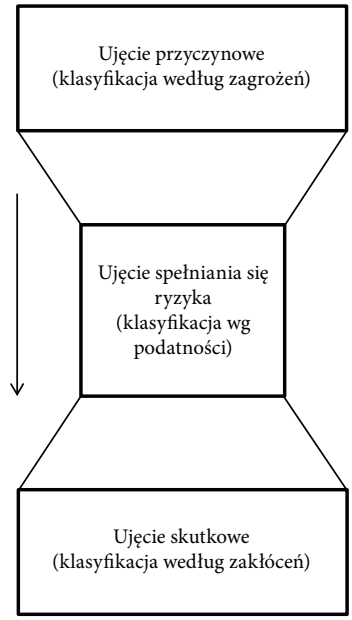
Dla celów prowadzanego procesu badawczego przyjęto kilka tez będących jednocześnie założeniami przy budowaniu modelu zależności pomiędzy bezpieczeństwem narodowym a zarządzaniem kryzysowym:

1. W ramach modelu kierowania bezpieczeństwem narodowym, stosując przyczynowo-skutkową klasyfikację ryzyka, można wyodrębnić obszar zarządzania kryzysowego oraz przypisać mu zakres przedmiotowy i metody (reguły) optymalizacji ekonomicznej realizowanych zadań.
2. W obszarze zarządzania kryzysowego można zdefiniować dwa powiązane ze sobą procesy, tj. proces zarządzania ryzykiem bezwarunkowym oraz proces zarządzania sytuacją kryzysową.
3. Realizowane w ramach zarządzania kryzysowego oddziaływanie na operatorów infrastruktury krytycznej (dalej IK) jest formą zarządzania ryzykiem bezwarunkowym rozumianym jako interakcja zagrożenia z podatnością podmiotu, który doświadcza ryzyka.
4. Włączenie zarządzania ryzykiem operacyjnym jako jednego z elementów zarządzania sytuacją kryzysową jest uprawnione, gdyż system zarządzania kryzysowego spełnia kryteria organizacji (jego elementy składowe, łącznie z zależnościami jakie pomiędzy nimi zachodzą, spełniają definicję systemu w ramach „nadsystemu", jakim jest kierowanie bezpieczeństwem narodowym). Ponadto cele tego systemu osiągane są poprzez realizację procesów, które mogą być zakłócane przez czynniki wewnętrzne i zewnętrzne.
5. Zarządzanie ryzykiem operacyjnym może być wykorzystane w ramach zarządzania sytuacją kryzysową w aspekcie działań:
   - zorientowanych na sprawność,
   - zorientowanych procesowo,
   - zorientowanych na logistykę,
   - zorientowanych na społeczne zaufanie.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

6. Istnieje dualizm postępowania w przypadku zarządzania sytuacją kryzysową polegający na konieczności jednoczesnego zarządzania ryzykiem warunkowym oraz powiązanym z nim ryzykiem operacyjnym.

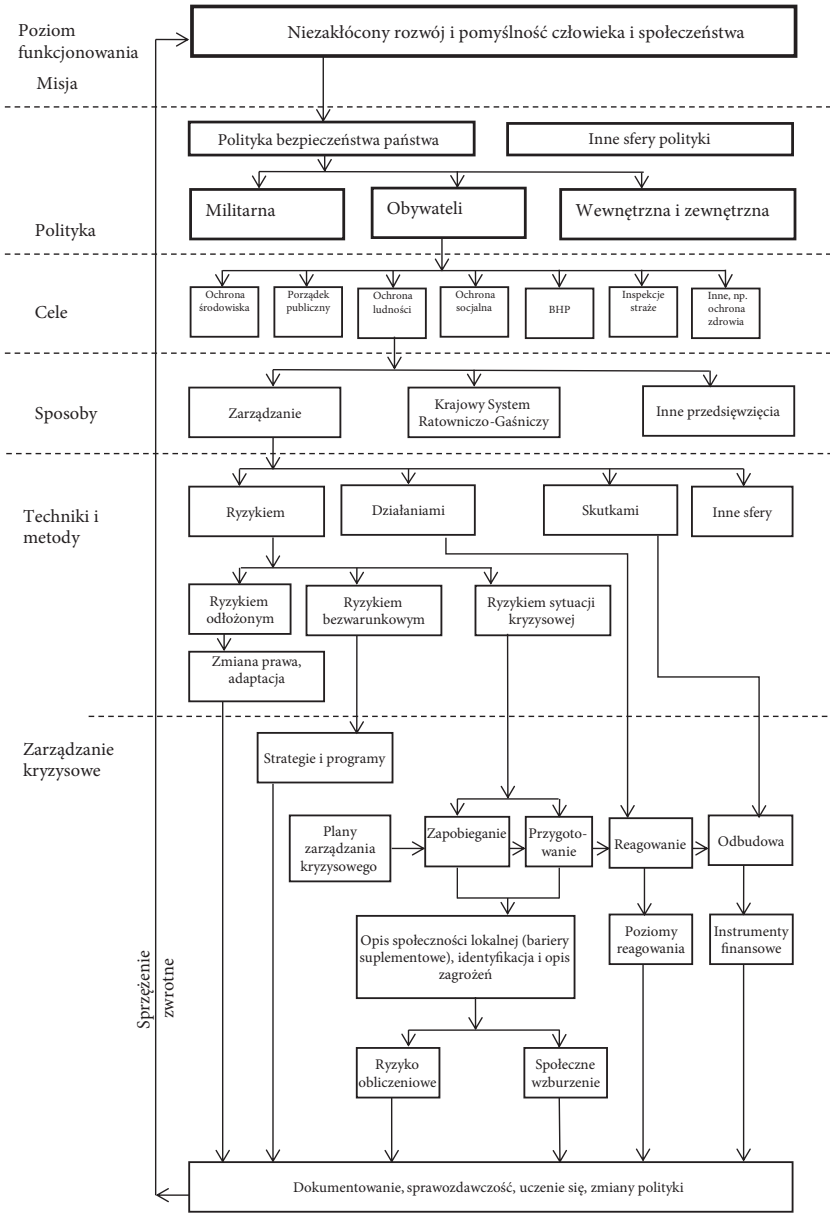
Wszystkie badane obszary są ze sobą powiązane poprzez jednolitą kwalifikację ryzyka, którą przedstawiono na rysunku nr 1:



Rys. 1. Model przyczynowo-skutkowy klasyfikacji ryzyka
Źródło: Zawiła-Niedźwiecki 2013, s. 40

Opierając się na wynikach analizy Raportu o zagrożeniach bezpieczeństwa narodowego (Uchwała Rady Ministrów nr 167/2015), przyjęto założenie, że istnieją dwa rodzaje zagrożeń. Są to zagrożenia statyczne (ciągłe) wykazujące niewielkie zmiany w czasie oraz zagrożenia dynamiczne, które wykazują się zmiennością. Zagrożenia statyczne generują ryzyko odłożone (np. skażenie środowiska powodujące zmiany w organizmach żywych dopiero w kolejnym pokoleniu, zmiany demograficzne mogące spowodować kryzys systemów emerytalnych po wielu latach itp.). Przeciwdziałanie takim zagrożeniom wiąże się z działalnością polityczną i legislacyjną. Natomiast zagrożenia dynamiczne w korelacji z ich spodziewanymi skutkami dają powiązane ze sobą ryzyko bezwarunkowe i warunkowe. Zarządzanie tymi rodzajami ryzyka wymaga podejmowania przez administrację publiczną planowych działań w aspekcie organizacyjnym, technicznym i finansowym. Wstępny model relacji pomiędzy bezpieczeństwem narodowym i zarządzaniem poszczególnymi kategoriami ryzyka przedstawiono na schemacie nr 1.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353



Schemat 1. Schemat funkcjonalno-strukturalnego modelu systemu bezpieczeństwa.
Źródło: opracowanie własne na podstawie: Wolanin 2005, s. 364

Przedstawiony na schemacie model wstępny zostanie poddany weryfikacji w dalszej części opracowania.

Zależności zachodzące pomiędzy badanymi obszarami w kontekście jednolitej kwalifikacji ryzyka przedstawiono w tabeli nr 1.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 1. Zależności zachodzące pomiędzy różnymi kategoriami ryzyka w kontekście ich jednolitej kwalifikacji

Typ zagrożenia	*Rodzaj ryzyka*	*Sposób zarządzania ryzykiem*	*Jednolita kwalifikacja ryzyka*	*Charakter zarządzania*	*Obszar wiedzy*
Stałe (ciągłe)	Odłożone	Długofalowe działania polityczne i legislacyjne	Ukierunkowane na przyczynę	Zarządzanie bezpieczeństwem narodowym	Nauki o bezpieczeństwie
Dynamiczne	Bezwarunkowe	Średnioterminowe strategie i programy	Ukierunkowane na podatność	Zarządzanie kryzysowe	Nauki właściwe z punktu widzenia zagrożenia np. – epidemiologia; – gospodarka wodna, – planowanie przestrzenne – nauki właściwe dla każdego z systemów infrastruktury krytycznej.
	Warunkowe	Krótko- i średnioterminowe plany i programy ukierunkowane na budowanie struktur i zasobów oraz utrzymanie ciągłości działania organizacji	Ukierunkowane na skutki społeczne	Zarządzanie sytuacją kryzysową, w tym ryzykiem operacyjnym, przy podejściu: – zorientowanym na sprawność; – zorientowanym procesowo; – zorientowanym na logistykę; – zorientowanym na społeczne zaufanie Zarządzanie ryzykiem operacyjnym obejmujące zarządzanie sprawnością systemu zarządzania kryzysowego (zagrożenia wewnętrzne).	Nauki o zarządzaniu

Źródło: opracowanie własne

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Strategia badawcza, charakter i zakres badań

W nauce powszechnie stosuje się dwa modele metodyczne: model hipotetyczno-dedukcyjny oraz model indukcji (Czakon 2006). W modelu hipotetyczno-dedukcyjnym na podstawie reguł wnioskowania logicznego dowodzi się prawdziwości wyjaśnienia. Z ogólnych teorii wywodzi się hipotezy, a następnie bada je na podstawie danych empirycznych. W przypadku indukcji, w odniesieniu do poznania empirycznego formułuje się początkowo niepewne propozycje (hipotezy), które za pomocą procesu badawczego mogą być zweryfikowane. Efektem końcowym jest uogólnienie.

Ze względu na charakter prowadzonego procesu badawczego oba te podejścia zostały połączone, przy czym podejście indukcyjne było traktowane jako zasadnicze, a dedukcja stanowiła element uzupełniający. W pierwszym etapie, na podstawie badań literaturowych przy wykorzystaniu podejścia systemowego, opisano obszar funkcjonowania zarządzania kryzysowego. Konieczność przeprowadzenia tego etapu dociekań wynikała z ubogiego dorobku literatury w odniesieniu do stosowania narzędzi zarządzania ryzykiem, a szczególnie ryzykiem operacyjnym, w odniesieniu do organizacji tworzonych przez administrację publiczną. Drugi etap badań miał charakter teoriotwórczy. Podejściem stosowanym w tej fazie było podejście procesowe. Jednocześnie zawartość rozdziałów i ich kolejność została oparta o wnioskowanie dedukcyjne. Polegało ono na takim przedstawieniu treści, by wynik badań jednego etapu był podstawą badań w kolejnym przy utrzymaniu następstwa logicznego.

Przyjęto wstępnie, że zasadniczym elementem w nowym podejściu teoretycznym jest uwzględnianie zarządzania ryzykiem operacyjnym jako nieodłącznej części zarządzania kryzysowego. Jednak na wstępie należało udzielić odpowiedzi na pomocnicze pytanie:

Przy jakich uwarunkowaniach struktury powoływane doraźnie w ramach administracji publicznej można uznać za organizacje?

Po weryfikacji tego zagadnienia można było przejść do zasadniczego celu dociekań w tej fazie. Aby wykazać istnienie związków pomiędzy zarządzaniem ryzykiem operacyjnym a zarządzaniem kryzysowym należało udzielić odpowiedzi na pytanie:

Jakie zależności występują pomiędzy ryzykiem operacyjnym a pozostałymi rodzajami ryzyka, którymi zarządza się w ramach publicznego zarządzania kryzysowego?

Prowadzone badania należy kwalifikować jednocześnie jako stosowane (praktyczne) oraz deskryptywne. Celem badań praktycznych jest sformułowanie nowych pragmatycznych wniosków, które mogą być wdrożone do praktyki w celu poprawy efektywności[6] działania. Natomiast w badaniach deskryptywnych fakty

[6] Pojęcia „efektywność", „sprawność" i „skuteczność" są wieloznaczne, dlatego nie zostały uwzględnione w definicjach przyjętych na potrzeby tego opracowania. Według T. Kotarbińskiego efektywność i skuteczność to kategorie szczegółowe pojęcia prakseologicznego – sprawność (Kotarbiński 1973, s. 127–142). Dla J. Zieleniewskiego skuteczność, korzystność i ekonomiczność to walory praktyczne sprawności (Zieleniewski 1975, s. 232–233). Z kolei skuteczność jest mierzona stosunkiem parametrów zrealizowanych do zaplanowanych efektów procesów, czyli określa zdolność do osiągnięcia

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

lub zjawiska przedstawia się pod kątem ich struktury i mechanizmów funkcjonowania (Nowosielski 2016).

Praca ma charakter teoretyczno-empiryczny, a jednocześnie multidyscyplinarny. Przedmiotem badań był system zarządzania kryzysowego będący elementem bezpieczeństwa narodowego. Ten obszar badawczy utożsamiany jest zazwyczaj z naukami o bezpieczeństwie w ramach obszaru nauk społecznych. Jednak postawiony problem badawczy dotyczy zagadnienia ryzyka operacyjnego związanego z zapewnieniem ciągłości działania organizacji. Budowanie i utrzymywanie bezpieczeństwa poprzez zarządzanie ryzykiem, w tym ryzykiem operacyjnym, jest działaniem typowym dla świata biznesu, głównie dla sektora bankowego i ubezpieczeniowego (Pilarczyk 2011). Podbudową naukową dla metod i praktyk związanych z zarządzaniem ryzykiem są nauki o zarządzaniu w dziedzinie nauk ekonomicznych w efekcie wynik dociekań prowadzonych w tym opracowaniu sytuuje się w naukach o zarządzaniu.

Mimo że badania były prowadzone na potrzeby praktyki (planowane wdrożenie elementów zarządzania ryzykiem do istniejącego systemu zarządzania kryzysowego), to znaczna ich część ma charakter badań poznawczych. Jest to wynikiem stosunkowo ubogiego dorobku literaturowego w odniesieniu do możliwości stosowania zdobyczy nauk o zarządzaniu w procesie postępowania z ryzykiem w ramach działalności administracji publicznej. W szczególności dostępna literatura nie pozwalała wyjaśnić, dlaczego poprawnie zdefiniowany system w konfrontacji z realnymi zdarzeniami niekiedy zawodzi lub wykazuje się efektywnością niższą od oczekiwanej. Ta początkowa niewiedza pozwoliła na sformułowanie zarówno celu badań, jak i głównego problemu badawczego.

Charakter prowadzonych badań, a zwłaszcza charakter pytania badawczego, determinuje dobór metod badawczych oraz sposób doboru przypadków wykorzystanych w metodzie case-study (Wójcik 2013). Celem dokonania wyboru typu badań właściwych na każdym z etapów prowadzonych dociekań posłużono się poniższą tabelą.

Tabela 2. Klasyfikacja celów badań ze względu na typ badań (kryterium przedmiotowe)

Typ badań	*Charakterystyka typu badań*	*Opis szczegółowy celu (celów)*
Badania podstawowe (teoretyczne)	Badania podstawowe polegają na formułowaniu ogólnych praw nauki. Opierając się na teoretycznych założeniach tych badań (typu poznawczego), rozpatruje się i wyjaśnia problemy (zagadnienia) określonej teorii naukowej lub koncepcji.	Teoretyczne wzbogacenie wiedzy danej dziedziny lub dyscypliny poprzez odkrywanie nowych prawd, związków zachodzących między zjawiskami, tworzenie podbudowy teoretycznej i opracowywanie nowych teorii.

zamierzonych celów (Stoner, Wankel 1992, s. 170–171). Jednocześnie, według Pszczółkowskiego, jeżeli cel nie został osiągnięty, działanie jest wówczas nieskuteczne. Jeżeli jednak w wyniku określonego działania otrzymywane są rezultaty cenne, chociaż niezamierzone, działanie takie jest efektywne (efektem jest wynik pozytywny, niekoniecznie związany z celem) (Pszczołowski 1982a, s. 159; Pszczołowski 1982b, s. 249). Działanie nieskuteczne może być więc efektywne, jeżeli związane są z nim wyniki pozytywne. Stąd każde działanie skuteczne jest efektywne, efektywne natomiast nie musi być skuteczne.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Typ badań	*Charakterystyka typu badań*	*Opis szczegółowy celu (celów)*
Badania stosowane (praktyczne)	Badania stosowane to przede wszystkim badania empiryczne. Prace badawcze na potrzeby praktyki to najczęściej prace empiryczne mające charakter prac deskryptywnych (opisowych), eksplanacyjnych (wyjaśniających) i replikacyjnych (powtórzeniowych).	Sformułowanie nowych pragmatycznych wniosków, które mogą być wdrożone do praktyki w celu poprawy efektywności działania. Dotyczą zmian organizacyjnych, w tym nowych stylów zarządzania.
Badania stosowane deskryptywne	Badane fakty lub zjawiska przedstawia się pod kątem ich struktury i mechanizmów funkcjonowania. Pytania problemowe w tych badaniach zaczynają się od zaimka: „jaka", „jaki", „która". Są to zatem przeważnie pytania dopełnienia.	Opis struktury i/lub mechanizmów funkcjonowania badanych obiektów i zjawisk.
Badania stosowane eksplatacyjne	Prace eksplanacyjne ujmują badania związków i zależności przyczynowych między określonymi zjawiskami. W badaniach stosuje się przeważnie pytania rozstrzygnięcia.	Zidentyfikowanie i wyjaśnienie relacji (zależności) między określonymi zmiennymi.
Badania stosowane replikacyjne	Prace replikacyjne, z reguły odtwórcze, przedstawiany w nich problem badawczy był już przez innych badany wcześniej. Rozszerzają one uprzednie badania lub też mogą być przeprowadzane innymi metodami. Stosuje się pytania zarówno dopełnienia, jak i rozstrzygnięcia.	Poszukiwanie potwierdzenia lub różnicy w badanym uprzednio zjawisku lub procesie. Tworzenie nowych hipotez.

Źródło: S. Nowosielski 2016, s. 472

Dobór metod badawczych

Wśród zastosowanych metod empirycznych wyróżnić należy obserwację bezpośrednią (w tym obserwację uczestniczącą), zaś wśród metod teoretycznych – analizę, syntezę i analogię. Dla omawianego procesu zasadnicze znaczenie miały cztery metody: dedukcja, indukcja, badania w działaniu (*action research*) oraz studium przypadku (*case study*).

1. Dedukcja

Jest to metoda, która polega na przechodzeniu od ogółu do szczegółu. Wykorzystując wiedzę o całości, wnioskujemy o niektórych częściach składowych (elementach, przedmiotach) z danej całości (Apanowicz 2002).

2. Wnioskowanie indukcyjne

To takie wnioskowanie, w którym na podstawie wielu przesłanek jednostkowych, stwierdzających, iż poszczególne zbadane przedmioty pewnego rodzaju

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

mają pewną cechę, dochodzi się (przy braku przesłanek negatywnych) do wniosku ogólnego, że każdy przedmiot tego rodzaju taką cechę posiada (Ziembiński 1997).

3. Badania w działaniu (*action research*)

Action research to grupa metod badawczych mieszcząca się w obszarze badań jakościowych. Dla potrzeb niniejszego opracowania zastosowano jedną z nich występującą pod nazwą „badania uczestniczące" (*parcticipatory action research*). Kluczowe w tym podejściu jest włączanie niektórych członków organizacji do procesu badawczego, a nie tylko sprowadzanie ich do roli obiektów poddawanych analizie (Ćwiklicki, Pawlina 2015). Równocześnie jest to rodzaj badania, w którym bliska współpraca z obiektem badań i praktyczne rozwiązanie problemu jest częścią procesu badawczego (Eriksson, Kovalainen 2008), w ślad za (Ćwiklicki 2014). Celem tej metody jest opisanie i zrozumienie zjawiska, a nie przewidywanie zdarzeń przyszłych czy kontrola ich przebiegu (MacDonald 2012). W efekcie dla *action research* właściwe jest zastosowanie mające na celu rozwiązanie konkretnego problemu niż rozwoju teorii (Ćwiklicki 2014). W ujęciu praktycznym stosowanie tej metody polega na tym, że badacz identyfikuje sytuację, określa wstępną propozycję usprawnień i metodykę postępowania. Jako aktywny uczestnik działania ma również możliwość oceny efektów zastosowanych rozwiązań i proponowania korekty. Jednocześnie badani aktywnie uczestniczą we wszystkich fazach procesu badawczego. Są partnerami badacza na etapie diagnozy sytuacji i oceny efektów podjętej interwencji (Ćwiklicki, Pawlina 2015). Proces badawczy prowadzony tą metodą jest zgodny ze schematem: plan (zdiagnozowanie sytuacji przy udziale badanych) – działanie (przeprowadzenie zmiany) – refleksja (obserwacja efektów wprowadzonej interwencji). W kolejnym cyklu (cyklach) powtarza się wcześniejsze etapy.

4. Studium przypadku (*case study*)

Studium przypadku to szczegółowy opis, zazwyczaj rzeczywistego, zjawiska gospodarczego, np. organizacji, procesu zarządzania, jego elementów lub otoczenia organizacji, w celu sformułowania wniosków o przyczynach i rezultatach jego przebiegu (Grzegorczyk 2015). Jest to jakościowa metoda badań szczególnie przydatna, kiedy celem jest poznanie okoliczności i przyczyn występowania danego zjawiska oraz określenie relacji między zjawiskami (Wójcik 2013). Wg J. Zieleniewskiego (Zieleniewski 1975) jest to najbardziej „unaukowiona" droga dojścia od etapu obserwacji funkcjonowania instytucji, poprzez uogólnione hipotezy, aż do ogólnych twierdzeń. Posługując się tą metodą, należy na podstawie doświadczenia życiowego dokonać wyboru konkretnych, indywidualnych przypadków i przeprowadzić ich badanie, analizując funkcjonowanie całych instytucji lub wybranych fragmentów. W procesie badawczym wykorzystano przypadki uważane za najbardziej typowe dla danej sytuacji, a jednocześnie pozwalające na możliwie precyzyjny opis. Równocześnie przy wyborze analizowanych przypadków stosowano podejście sytuacyjne, które zakłada relatywizm zasad i reguł organizacyjnych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Podejście to przyjmuje, że zasady i reguły organizacyjne mają zastosowanie ograniczone jedynie do pewnych klas sytuacji.

Użycie metody studium przypadku jest rekomendowane w celu znalezienia odpowiedzi na pytania mające charakter odkrywczy, a więc dotyczące tego, „jak" i „dlaczego" dane zjawisko występuje (Yin 1994). Najważniejszym elementem przy stosowaniu tej metody jest ustalenie ilości przypadków, które mają być badane. W metodach ilościowych dąży się do uzyskania próby reprezentatywnej. W metodach jakościowych należy dążyć do uzyskania próby celowej. W przypadku falsyfikacji wystarczającym jest jeden przypadek, gdyż jak wykazał Karl Popper, dowolna ilość przypadków nie pozwala dowieść, że wszystkie łabędzie są białe. Wystarczy jednak jeden przypadek by dowieść, że jest to nieprawda (Popper 1959). Celem rozwiązywania problemów z zakresu nauk o zarządzaniu przy pomocy metody *case study* można przeprowadzić badanie pojedynczego lub wielokrotnego studium przypadku. Pierwszy wariant jest stosowany m.in. wtedy, gdy badane zjawisko ma charakter odkrywczy (teoriotwórczy) (Wójcik 2013).

Tabela 3. Typy studiów przypadku w zależności od celu badawczego

	Liczba studiów przypadku	
Jednostki analizy	1	>1
Holistyczne	Cel: odkrycie teorii (podejście indukcyjne) lub falsyfikacja Cel: potwierdzenie teorii (podejście dedukcyjne)	Cel: testowanie teorii (podejście dedukcyjne); porównanie przypadków między sobą
Zagnieżdżone	Cel: falsyfikacja Badanie wyłącznie procesów, jednostek lub projektów w ramach większego przypadku	Cel: testowanie lub poprawa teorii (podejście dedukcyjne) Porównanie jednostek (kategorii) o kontrastujących cechach w ramach większego przypadku

Źródło: Wójcik 2013; na podstawie: Yin 1994, s. 46

Wybór konkretnych przypadków powinien być dokonywany pod kątem m.in. specyficznych cech odmiennych od głównego nurtu grupy przypadków (Pizło 2009). Aby to osiągnąć można posłużyć się metodą podziału stratygraficznego (Shakir 2002). Metoda polega na ustaleniu cech, jakie powinny mieć badane przypadki. W kolejnym kroku tak dobiera się przypadki do badania, by każda cecha była reprezentowana wymaganą ilość razy. W efekcie uzyskuje się próbę docelową (Riche, Lewis 2003), (Miles, Huberman, Saldaña 2014). Biorąc pod uwagę, że w części empirycznej badania oparte o *case study* miały wskazywać wskazywać poprawność przyjętej tezy, w ślad za (Czakon 2006) przyjęto, że dla każdego wprowadzonego założenia oraz dla każdego obszaru badawczego należy wskazać minimum 4 przypadki, które następnie poddano szczegółowej analizie. Dobór przypadków w postaci tabeli stratygraficznej przedstawiono w załączniku nr 1.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zakres badań

Przedmiotem badań był system zarządzania kryzysowego, powołany do życia na bazie ustawy o zarządzaniu kryzysowym (tekst jedn. DzU z 2017 r. poz. 209, art. 3 pkt. 1, dalej UZK) oraz zadania i elementy organizacyjne wynikające z UMOL. Ponieważ decyzja UMOL nie została jeszcze wdrożona do praktyki administracji publicznej w Polsce, elementy z nią związane potraktowano postulatywnie. W warstwie językowej gdy w odniesieniu do UZK zastosowano określenia „zapewnia", „umożliwia" itp., to w odniesieniu do UMOL stosowano określenia „powinno zapewnić", „powinno umożliwić".

W procesie badawczym dominującym podejściem było podejście systemowe. Podejście takie wiązało się z traktowaniem badanego przedmiotu jako pewnego systemu. Podejście to zostało uzupełnione o podejście procesowe postrzegające organizację działalności jako zbudowanej na bazie naturalnych procesów. Dodatkowo stosowano kilka innych podejść, a mianowicie: podejście historyczne (jaki był dotychczasowy rozwój badanego zjawiska w Polsce i wybranych państwach), podejście informacyjne (kładące nacisk na przepływy informacji), organizacyjno-prawne (uwzględniające istniejące struktury organizacyjne oraz przepisy prawa). Szczególnie ważnym obszarem analizy systemu zarządzania kryzysowego były aspekty funkcjonalno-czynnościowe prowadzone w następujących ujęciach:

- jako element „nadsystemu", jakim jest system kierowania bezpieczeństwem narodowym;
- w ujęciu podmiotowym z punktu widzenia zagadnień, na które zarządzanie kryzysowe oddziałuje (bezpieczeństwo ludzi, mienia i środowiska oraz dodatkowo infrastruktura krytyczna);
- w ujęciu przedmiotowym, w którym przedmiotem badań jest sama administracja publiczna, zaś zarządzanie kryzysowe ma uzupełniać jej możliwości działania w przypadku wystąpienia nieadekwatności sił i środków.

Szczególny nacisk został położony na te zagadnienia, które wiążą się z zarządzaniem ryzykiem i przygotowaniem reakcji na wypadek zmaterializowania się ryzyka. Przyjęto, że system powinien reagować również na te rodzaje ryzyka, którymi administracja nie zarządza, oraz na zagrożenia, których wcześniej nie przewidywano.

Struktura pracy

Na potrzeby niniejszego opracowania autor przeanalizował przypadki aktywowania systemu zarządzania kryzysowego, protokoły z posiedzeń Rządowego Zespołu Zarządzania Kryzysowego, materiały przekazywane w ramach spotkań roboczych *High Level Risk* Forum prowadzonego w ramach Organizacji Współpracy Gospodarczej i Rozwoju (OECD) oraz wiele danych literaturowych dotyczących sytuacji kryzysowych, jakie wystąpiły zarówno w Polsce, jak i w innych krajach.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Praca składa się z wprowadzenia zawierającego kontekst badawczy, sześciu rozdziałów zasadniczych oraz zakończenia.

We wprowadzeniu przedstawiono cel i zakres pracy oraz wykaz podstawowych pojęć stosowanych w opracowaniu wraz z ich definicjami.

W rozdziale pierwszym opisano system zarządzania kryzysowego w ujęciu formalno-prawnym, w tym cykle i procesy, jakie wynikają z obowiązujących przepisów. Główny nacisk w tym rozdziale został postawiony na cykl zarządzania kryzysowego oraz strukturę organizacyjną badanego systemu.

W rozdziale drugim przedstawiono powiązania pomiędzy administracją publiczną a podmiotami (w tym podmiotami gospodarczymi) dostarczającymi usługi kluczowe z punktu widzenia zarówno obywateli, jak i państwa jako całości. Szczególna uwaga została zwrócona na wspólne procesy realizowane przez podmioty administracji publicznej i operatorów infrastruktury krytycznej (IK).

W rozdziale trzecim przedstawiono zarządzanie kryzysowe (ZK) w ujęciu systemowym oraz z punktu widzenia zarządzania społecznymi skutkami zagrożenia. Ponadto przeanalizowano różnice w definiowaniu zarządzania kryzysowego w ramach nauk o bezpieczeństwie oraz w ramach nauk o zarządzaniu.

W rozdziale czwartym przeanalizowano różne formy zarządzania ryzykiem w administracji publicznej. Najważniejszym elementem badań prowadzonych w tej części pracy były zagadnienia ujęcia systemowego i procesowego w odniesieniu do funkcji stosowanych lub wdrażanych do stosowania, w ramach publicznego zarządzania kryzysowego.

W rozdziale piątym zostało wskazane miejsce zarządzania ryzykiem operacyjnym w publicznym zarządzaniu kryzysowym jako powiązanego z ryzykiem warunkowym i ryzykiem wystąpienia sytuacji kryzysowej. Ponadto przedstawiono możliwości stosowania elementów ekonomiki w ramach zarządzania poszczególnymi rodzajami ryzyka.

W rozdziale szóstym przedstawiono możliwości zarządzania ryzykiem wystąpienia sytuacji kryzysowej z punktu widzenia zarządzania podatnością oraz zarządzania przyczyną.

W zakończeniu dokonano podsumowania prowadzonych rozważań, przedstawiono wnioski oraz wskazano obszary, które zdaniem autora wymagają dalszych poszerzonych badań.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rozdział I
Elementy zarządzania kryzysowego w administracji publicznej

Elementem poprzedzającym badanie danej organizacji jest ustalenie kontekstu, w jakim ona funkcjonuje. Wymaga to szczegółowej znajomości procesów realizowanych w organizacji oraz czynników wewnętrznych i zewnętrznych, jakie mają na nią wpływ (Matuszak-Flejszman, Pochyluk 2016). Badania w niniejszym rozdziale opierają się na podejściu historycznym (w celu ustalenia, w jaki sposób został ukształtowany system zarządzania kryzysowego) oraz na podejściu organizacyjno-prawnym. To drugie podejście ma zasadnicze znaczenie w odniesieniu do administracji publicznej, która bazuje na przepisach prawa. Celem tych badań jest określenie systemu zarządzania kryzysowego w ujęciu podmiotowym i przedmiotowym. Dodatkowo badania miały ujawnić przepływy informacji i decyzji w ramach systemu, co wymaga zastosowania podejścia informacyjnego.

Badania nawiązują do założenia nr 1 (w części dotyczącej opisania zakresu systemu zarządzania kryzysowego) oraz nr 4 (w odniesieniu do struktur istniejących w tym systemie oraz procesów realizowanych przez te struktury).

1.1. Proces kształtowania zarządzania kryzysowego w polskim systemie prawnym

Za początek procesu budowania zarządzania kryzysowego w administracji publicznej wskazuje się rok 1995, kiedy to dla Australii i Nowej Zelandii został wydany pierwszy standard zarządzania kryzysowego na poziomie krajowym (AS/NZS 4360 *Risk Management – Standards Australia and Standards New Zealand*). Z czasem podobne standardy zaczęły być stosowane w innych krajach. Administracja rządowa w Polsce bardzo długo nie uwzględniała w swoich zadaniach tych zagadnień. W odniesieniu do niekorzystnych zdarzeń jej działania na ogół sprowadzały się do powoływania i utrzymywania specjalistycznych służb (Państwowa Straż Pożarna, Policja, itp.), ewentualnie do opracowywania planów zwalczania danego zagrożenia (plany przeciwepidemiczne, przeciwpowodziowe, itp.). Nie istniało również systemowe podejście do zarządzania ryzykiem. Samo określenie „ryzyko" w krajowych aktach prawnych dotyczyło zagadnień związanych z ryzykiem w pracy (tj. z czynnikami mogącymi zagrozić życiu i zdrowiu pracownika) i działalności instytucji finansowych. W szerszym rozumieniu

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

pojęcie „ryzyko" pojawiło się dopiero w 2007 r. wraz dyrektywą unijną w sprawie oceny ryzyka powodziowego i zarządzania nim, gdzie zawarto następującą definicję: „ryzyko powodziowe oznacza kombinację prawdopodobieństwa wystąpienia powodzi i związanych z powodzią potencjalnych negatywnych konsekwencji dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej" (DzUrz UE L 288/27, art. 2 pkt. 2).

Włączenie zarządzania ryzykiem do praktyki administracyjnej jest związane z budowaniem systemu zarządzania kryzysowego. Proces ten został zapoczątkowany w wyniku powszechnej krytyki działań administracji publicznej w czasie tragicznej powodzi w 1997 r. Początkowo na szczeblu Rady Ministrów powstał Międzyresortowy Zespół Zarządzania Kryzysowego, natomiast w listopadzie 1998 r. Minister Spraw Wewnętrznych i Administracji powołał Urząd Zarządzania Kryzysowego i Ochrony Ludności jako jednostkę obsługującą Szefa Obrony Cywilnej Kraju (Podolski 2010). Podstawą do przygotowania szerszych regulacji ustawowych były prace prowadzone w Instytucie Spraw Publicznych i prezentowane w formie raportów. W jednym z nich (Stec, Płoskonka, Prutis 1999) autorzy nakreślili podstawowe zasady organizacji systemu zarządzania kryzysowego w Polsce. Początkowo opierano się na określeniu „nadzwyczajne zagrożenie". W raporcie z badań znalazła się następująca definicja tego pojęcia: „Do nadzwyczajnych zagrożeń należą takie zjawiska przyrody jak: powodzie, zatopienia, huragany, gradobicia, susze, oberwania chmury oraz wiele zagrożeń związanych z działalnością człowieka. Do podstawowych z nich należą zagrożenia skażeniem radiacyjnym, wybuchami gazu, epidemie, katastrofy komunikacyjne czy budowlane, pożary, terroryzm czy zakłócenia porządku publicznego" (Stec, Płoskonka, Prutis 1999, s. 5). Jednocześnie w dalszej części tego samego raportu zamiast terminu „nadzwyczajne zagrożenie" stosuje się pojęcie „sytuacja kryzysowa". Według autorów „nadzwyczajne zagrożenie" oraz „stan kryzysu" mogą błędnie kojarzyć się z koniecznością wprowadzenia stanu nadzwyczajnego. Dlatego, ich zdaniem, już w fazie nazewnictwa należy zdecydowanie różnicować pojęcia związane z zagrożeniami (np. klęska żywiołowa) od pojęć definiujących stan prawny, w jakim funkcjonują organy administracji publicznej (przywołana wcześniej klęska żywiołowa jest jedynie jedną z przesłanek wprowadzenia stanu klęski żywiołowej). Pomimo tej deklaracji autorom reformy z 1999 r. nie udało się wprowadzić określenia „sytuacja kryzysowa" do systemu prawnego. Dodatkowo autorzy reformy określili zasady, które miały zapewnić poprawę skuteczności reagowania administracji na zdarzenia nadzwyczajne. Te zasady to:

- zasada prymatu układu terytorialnego,
- zasada jednoosobowego kierownictwa i odpowiedzialności,
- zasada kierowania i ponoszenia odpowiedzialności przez jednoosobowe organy sprawujące władzę administracji ogólnej,
- zasada adekwatności (dotyczy właściwego szczebla administracyjnego reakcji),

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

- zasada powszechności,
- zasada oddzielenia systemu gotowości cywilnej od systemu gotowości militarnej.

Te zasady (z wyjątkiem ostatniej) zostały ostatecznie zawarte w UZK uchwalonej dopiero w 2007 r. W jej pierwotnym brzmieniu (DzU z 2007 r. nr 89, poz. 590, art. 3 pkt 1) ilekroć mowa o sytuacji kryzysowej, „należy przez to rozumieć sytuację będącą następstwem zagrożenia i prowadzącą w konsekwencji do zerwania lub znacznego naruszenia więzów społecznych przy równoczesnym poważnym zakłóceniu w funkcjonowaniu instytucji publicznych, jednak w takim stopniu, że użyte środki niezbędne do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych, o których mowa w art. 228 ust. 1 Konstytucji Rzeczypospolitej Polskiej".

W praktyce, aby sytuacja taka zaistniała, konieczne było jednoczesne spełnienie kilku czynników:

- istnienie zagrożenia,
- zerwanie lub znaczne naruszenie więzów społecznych,
- poważne zakłócenie w funkcjonowaniu instytucji publicznych,
- brak przesłanek do wprowadzenia stanu nadzwyczajnego.

Tak sformułowana definicja została zaskarżona do Trybunału Konstytucyjnego. Ten uznał definicję sytuacji kryzysowej za niezgodną z art. 2 Konstytucji RP. Jednocześnie orzekł, że przepis traci moc obowiązującą po upływie 12 miesięcy od daty opublikowania wyroku w Dzienniku Ustaw (K 50/07, DzU z 2009 r. nr 65, poz. 553). Odpowiedzią na ten wyrok była dogłębna nowelizacja ustawy (DzU z 2009 r. nr 131, poz. 1076), w tym zmiana zakwestionowanej definicji. Ostatecznie do systemu prawnego trafiła następująca definicja: „Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej" (UZK, art. 2). Jednocześnie wspomniana sytuacja kryzysowa to: „Sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków" (UZK, art. 3 pkt 1).

Natomiast do stwierdzenia, że mamy do czynienia z sytuacją kryzysową (UZK, art. 3) niezbędne jest zaistnienie jedynie dwóch elementów:

- sytuacji wpływającej negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska;
- znacznego ograniczenia w działalności właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Innymi słowy, dopóki siły i środki organu właściwego do zwalczania zagrożenia (bądź łagodzenia jego skutków) są wystarczające, nie ma mowy o wystąpieniu sytuacji kryzysowej, bez względu na charakter czy rozmiar istniejącego zagrożenia. Przytoczona powyżej definicja jest istotna, gdyż to nie wielkość i dolegliwość zdarzenia, lecz „ograniczenie w działaniu organów administracji publicznej" jest podstawowym czynnikiem decydującym, czy zdarzenie jest kryzysowe bądź nim nie jest. To zwrócenie uwagi na aspekt funkcjonalny przybliża zarządzanie kryzysowe do nauk o zarządzaniu (Krzyżanowski 1994), zaś konieczność utrzymania sprawności działania organów administracji poddanych presji kryzysu sugeruje możliwość stosowania narzędzi znanych w zarządzaniu ryzykiem operacyjnym.

Zmiany w podstawach prawnych związanych z zarządzaniem kryzysowym są również warunkowane pracami, jakie toczą się na forum międzynarodowym, głównie ONZ i Unii Europejskiej. We wstępie wspomniano już o wejściu w życie UMOL, który stopniowo staje się prawem obowiązującym we wszystkich krajach członkowskich UE. Jego znaczenie dla problematyki zarządzania ryzykiem będzie omawiane w dalszej części opracowania. Drugim źródłem spodziewanych zmian są prace prowadzone na forum ONZ, a związane z ograniczaniem skutków zmian klimatu. W ramach tych prac zorganizowana przez ONZ Światowa Konferencja na temat Zapobiegania i Ograniczania Skutków Katastrof w swoim raporcie (*Report of the World Conference on Disaster Reduction*) przyjęła „Plan działania z Hyogo na lata 2005–2015" (*Hyogo Framework for Action 2005–2015*). W ramach planu postanowiono poprawić zdolności do reagowania na wypadek wystąpienia katastrofy, zapewnić koordynację działań i współpracę międzynarodową. Po zakończeniu realizacji planu kolejna konferencja, tym razem poświęcona sprawie redukcji ryzyka katastrof (*Third UN World Conference on Disaster Risk Reduction*), przyjęła nowy dokument strategiczny pt. „Ramy działania z Sendai na rzecz redukcji ryzyka katastrof" (*Sendai Framework for Disaster Risk Reduction 2015–2030*). Tym razem akcent postawiono na zapobieganiu klęskom żywiołowym na podstawie oceny i zarządzania ryzykiem.

1.2. Zakres zadań realizowanych w ramach zarządzania kryzysowego

UZK nie zawiera definicji kryzysu. Pominięcie tego pojęcia nie jest przypadkowe. Spośród wielu dostępnych definicji można przytoczyć następujące:

- kryzys to moment, okres przełomu, przesilenie, decydujący zwrot; okres załamania gospodarczego (Kopaliński 1989, s. 285);
- kryzys w sensie przedmiotowym to zerwanie istniejącego układu, polegające na zmianie jego struktury lub funkcji albo obu tych elementów łącznie (Wróblewski 1996, s. 9);
- kryzysem będziemy nazywali kulminacyjną fazę eskalacji zagrożenia, często całkowitą utratę kontroli nad zaistniałą sytuacją, w której następuje przełom (punkt zwrotny) jakiegoś procesu, w wyniku którego dany podmiot może ulec

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

likwidacji, destrukcji lub (uzyskać szansę – przyp. autora) powrotu do normalności, a nawet rozwoju (Marszałek, Sobolewski, Majchrzak 2012, s. 31).

I właśnie ta ostatnia definicja wyjaśnia najlepiej postawę administracji publicznej wobec możliwości zaistnienia kryzysu. Skoro w chwili kryzysu tracimy zdolność do zarządzania taką sytuacją, a jednocześnie grożą nam zmiany destrukcyjne, to celem nadrzędnym zarządzania kryzysowego jest takie pokierowanie rozwojem sytuacji, by do kryzysu nie dopuścić. Ten poddający się kontroli rozwój sytuacji został nazwany sytuacją kryzysową.

Zastosowana w ustawie definicja nie jest jedyną, jaka występuje w literaturze. Uwagę należy zwrócić na kilka z nich.

Z sytuacją kryzysową będziemy mieli do czynienia wówczas, gdy:

- przekroczony zostanie akceptowany przez dany podmiot poziom zagrożeń i następuje ich eskalacja (narastanie, wzrost) – często dochodzi do utraty kontroli nad przebiegiem wydarzeń;
- zaniechanie podjęcia działań (reagowania) może doprowadzić do kryzysu, jako kulminacyjnego elementu sytuacji kryzysowej, a w konsekwencji nawet do dezorganizacji danego systemu;
- rozwiązania zaistniałej sytuacji kryzysowej wymagają szczególnych działań oraz często dodatkowych nakładów sił i środków (Marszałek, Sobolewski, Majchrzak 2012, s. 2–29).

Analizując problematykę sytuacji kryzysowej, należy odpowiedzieć na pytanie: czy z chwilą wprowadzenia jednego ze stanów nadzwyczajnych (kwalifikowanych) zarządzanie kryzysowe kończy się, czy nie? Autor prezentowanego opracowania skłania się do przyjęcia następującego stanowiska: „Głównym celem wprowadzenia stanów nadzwyczajnych w państwie jest opanowanie sytuacji kryzysowej dla państwa i obywateli, której źródłem są zagrożenia kryzysowe o charakterze naturalnym, technicznym lub społecznym, w wyniku których oddziaływania może dojść do destabilizacji państwa i załamania równowagi funkcjonowania obywateli" (Marszałek, Sobolewski, Majchrzak 2012). Innymi słowy, wprowadzenie stanu nadzwyczajnego jest kolejnym, dodatkowym narzędziem zarządzania sytuacją kryzysową.

Skoro tak, to nie można pomijać najpoważniejszego zagrożenia dla bezpieczeństwa państwa, jakim są zagrożenia militarne i możliwości wprowadzenia stanu wojennego jako narzędzia do zwalczania takich zagrożeń. Ustawa w swoich założeniach wskazuje na dwa obszary integracji zarządzania kryzysowego z realizacją zadań obronnych. Jest to włączenie struktur zarządzania kryzysowego do systemu kierowania bezpieczeństwem narodowym (praktyczny wymiar tej integracji to realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa) (DzU z 2004 r. nr 98, poz. 978) oraz obowiązek zaimplementowania zadań realizowanych w ramach systemu zarządzania kryzysowego NATO do obowiązków poszczególnych organów administracji rządowej. Jednak integrację krajowego i NATO-wskiego systemu

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

zarządzania kryzysowego komplikuje odmienne znaczenie pojęcia „zarządzanie kryzysowe". W rozumieniu NATO każde działanie niebędące obroną kolektywną jest realizowane w ramach zarządzania kryzysowego. Te działania mogą w skrajnym przypadku oznaczać prowadzenie wojny nazywanej kryzysem polityczno-militarnym. Jest to zatem zagadnienie zupełnie odmienne od „nieadekwatności środków" charakteryzującej sytuację kryzysową w rozumieniu UZK.

W rzeczywistości omawiane dwa obszary (zarządzanie kryzysowe i obrona narodowa) mają więcej elementów wspólnych. Raport o zagrożeniach bezpieczeństwa narodowego obejmuje zagrożenia militarne i terrorystyczne obok zagrożeń „cywilnych". W ramach UZK planuje się zarówno udział SZ RP w działaniach kryzysowych, jak i wsparcie, jakie tym siłom będzie udzielane przez administrację. Stopnie alarmowe mogą służyć podniesieniu ochrony zarówno jednostek wojskowych, jak i obiektów administracji rządowej. Jednak zmiana środowiska bezpieczeństwa powoduje, że ta integracja powinna być o wiele szersza. Stosowana wielokrotnie przez Rosję wojna hybrydowa (Gruzja, Ukraina) (Wojnowski 2014) i towarzysząca jej zmasowana propaganda (Wojnowski 2015) powodują, że kraje poddane naciskom rezygnują z wypowiadania wojny i ogłaszania stanu wojennego w obawie o nieprzychylne reakcje społeczności międzynarodowej. W konsekwencji zamiast klasycznej i formalnie wypowiedzianej wojny mamy różne formy „operacji antyterrorystycznej"[1] prowadzonej przez siły zbrojne, ale w ramach odpowiedzialności resortu spraw wewnętrznych. Pojawienie się tej nowej sytuacji powoduje, że pojawiają się głosy, by w miejsce zarządzania kryzysowego wprowadzić zarządzanie bezpieczeństwem poprzez zmodyfikowanie UZK, zmianę Rządowego Zespołu Zarządzania Kryzysowego na Komitet Rady Ministrów ds. Bezpieczeństwa Narodowego, zaś RCB w Rządowe Centrum Bezpieczeństwa Narodowego (Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej). Te postulaty nie przekształciły się jak dotychczas w projekt nowych regulacji ustawowych.

1.3. Fazy zarządzania kryzysowego

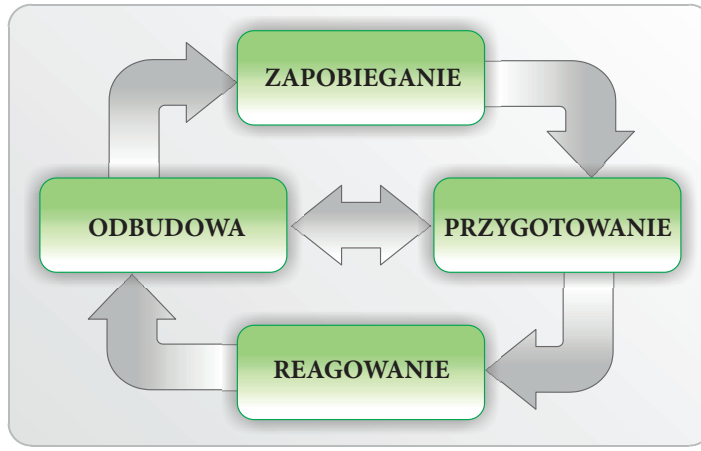
Aby działania administracji publicznej były skuteczne, nie mogą być podejmowane dopiero wówczas, gdy zdarzenie ma miejsce lub prawdopodobieństwo jego wystąpienia jest wysokie. Tym bardziej nie można czekać, aż okoliczności zagrożenia osiągną cechy sytuacji kryzysowej. Również ustąpienie bezpośredniego zagrożenia nie oznacza jeszcze, że administracja jest zwolniona z działań ograniczających długofalowe skutki zdarzenia. Ponieważ metody postępowania różnią się w zależności od tego, czy zagrożenie jest jedynie potencjalne, właśnie wystąpiło, czy mamy do czynienia z usuwaniem jego skutków, kompleksowe zarządzanie kryzysowe wyróżnia cztery fazy (UZK, art. 2). Są to:

[1] Zob. szerzej: *Operacja antyterrorystyczna na wschodzie Ukrainy*, http://www.defence24.pl/75436,operacja-antyterrorystyczna-na-wschodzie-ukrainy [dostęp 24.01.2016].

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

- zapobieganie,
- przygotowanie,
- reagowanie,
- usuwanie skutków, odtwarzanie zasobów i odtwarzanie IK (całość tych działań w literaturze nazywana jest odbudową (Augustyn 1998)).

W ujęciu całościowym wyżej wymienione fazy obejmują wszelkie działania zmierzające do eliminacji zagrożeń, przygotowania na ich wystąpienie, właściwą reakcję po zdarzeniu oraz działania przywracające stan sprzed zagrożenia. Zależności pomiędzy tymi fazami przedstawia schemat nr 2.



Schemat 2. Fazy zarządzania kryzysowego
Źródło: Skomra 2016, s. 60

Jak wynika z powyższego schematu, poszczególne fazy nie muszą występować kolejno po sobie. W fazie odbudowy należy pamiętać o odtwarzaniu zasobów zużytych w fazie reagowania, ale jednocześnie zasoby niewykorzystane do reagowania mogą być wykorzystywane w fazie odbudowy. Dodatkowo każda sytuacja kryzysowa powinna stanowić przesłankę do podjęcia działań zapobiegawczych i modernizacyjnych.

Oczywiście nie wszystkie te działania przypisane są administracji publicznej. Część ryzyka może być przenoszona na firmy ubezpieczeniowe, przez co koszty związane z odbudową nie muszą w całości obciążać ani osób poszkodowanych, ani budżetu państwa. Ponadto za część tych działań w rzeczywistości odpowiedzialność ponoszą sami obywatele lub ich nieformalne i formalne związki.

Dużą trudnością dla decydentów realizujących powyższe zadania jest fakt, że zapobieganie zagrożeniom, przygotowanie na wypadek sytuacji nadzwyczajnych, reagowanie i elementy odbudowy rozproszone są w różnych ustawach, w zależności od źródła zagrożenia. Przykładem takich rozwiązań może być ustawa o ochronie przeciwpożarowej (prewencja pożarowa) czy ustawa o zapobieganiu

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (szczepienia ochronne) (DzU z 2016 r. poz. 1866, rozdz. 4). UZK rozwiązań tych nie może ani zastępować, ani dublować. Biorąc pod uwagę powyższe uwarunkowania, UZK uwzględnia wyżej wymienione fazy wyłącznie w odniesieniu do sytuacji kryzysowej. Analizując zadania poszczególnych organów zarządzania kryzysowego (UZK, art. 14, 17 i 19), można zauważyć, że zostały one ograniczone do monitorowania, planowania, reagowania i usuwania skutków zagrożeń. Faza zapobiegania została pominięta. W fazie przygotowania przewidziano jedynie dwa zadania, tj. monitorowanie zagrożeń oraz działania planistyczne. Jedynie fazy reagowania i usuwania skutków zdarzeń wymieniono jako realizowane w całości odpowiednio pod kierownictwem wojewody, starosty i wójta.

1.3.1. Faza pierwsza – zapobieganie

W ustawie o zarządzaniu kryzysowym definicji zapobiegania nie ma. Znajduje się ona natomiast w UMOL i oznacza „wszelkie działania służące ograniczaniu ryzyka lub łagodzeniu negatywnych następstw klęsk lub katastrof dla ludzi, środowiska naturalnego oraz mienia, w tym dziedzictwa kulturowego" (art. 4, pkt 4). Jest to więc definicja bardzo ogólna, zakładająca, że zapobieganie to wszystkie działania, które przyczyniają się do redukcji ryzyka poprzez zmniejszenie prawdopodobieństwa wystąpienia klęski lub katastrofy, jak również takie, dzięki którym można ograniczyć negatywne skutki w przypadku ich wystąpienia.

Podstawową metodą zapobiegania przyszłym zdarzeniom jest eliminowanie źródeł zagrożenia. Jest to realizowane głównie poprzez stanowienie prawa (np. przepisy budowlane, przeciwpożarowe, regulację ruchu drogowego itp.) oraz tworzenie systemów jego egzekwowania. To zadanie jest zatem domeną szczebla centralnego administracji rządowej. Jednak eliminowanie zagrożeń nie jest jedyną metodą zapobiegania sytuacji kryzysowej. Trzymając się definicji tej sytuacji, należy zwrócić uwagę, że nieadekwatność w reagowaniu może być spowodowana nie tylko skalą czy charakterem zdarzenia, ale również brakiem właściwych procedur lub brakiem koordynacji działań pomiędzy różnymi podmiotami. Biorąc pod uwagę powyższe, należy uznać, że zapobieganie sytuacjom kryzysowym to całokształt przedsięwzięć zmierzających do eliminacji potencjalnych zagrożeń oraz eliminacji sytuacji kryzysowych wynikających ze złego współdziałania poszczególnych służb (czyli takie techniczne, osobowe i szkoleniowe przygotowanie służb reagowania, by ich zdolność podjęcia działań była adekwatna do spodziewanych zdarzeń).

Zgodnie z roboczym dokumentem opracowanym w Rządowym Centrum Bezpieczeństwa pt. „Wskazówki do przygotowania (aktualizacji) planów zarządzania kryzysowego ministrów i kierowników urzędów centralnych"[2] najistotniejsze zadania realizowane w fazie zapobiegania obejmują:

[2] Wskazówki do przygotowania (aktualizacji) planów zarządzania kryzysowego ministrów i kierowników urzędów centralnych, RCB Warszawa 2012 – materiał niepublikowany.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

- przegląd stanu prawnego, procedur i zasobów,
- ocenę stanu bezpieczeństwa,
- przygotowanie projektów przepisów z zakresu zarządzania kryzysowego,
- realizację długofalowych działań w zakresie bezpieczeństwa.

1.3.2. Faza druga – przygotowanie

Jeżeli źródła zagrożenia nie da się w pełni wyeliminować, w celu uniknięcia sytuacji kryzysowej należy tak przygotować zasoby materiałowe, techniczne i organizacyjne, by udało się zapanować nad niekorzystnym rozwojem sytuacji. Służyć temu mają rezerwy państwowe, magazyny przeciwpowodziowe, rezerwy finansowe zarówno samorządu terytorialnego, jak i RM. Elementem przygotowań jest również edukowanie społeczeństwa tak, by osoby, które znajdą się w sytuacji zagrażającej ich zdrowiu, życiu bądź mieniu potrafiły podejmować racjonalne działania zmniejszające to zagrożenie.

Działania, które powinny być realizowane w fazie przygotowania, sprecyzowano we wspomnianych już „Wskazówkach…". Zgodnie z nimi do działań realizowanych w tej fazie należy:

- opracowanie siatki bezpieczeństwa;
- opracowanie, uzgodnienie i aktualizacja planu zarządzania kryzysowego;
- wymiana bieżących informacji o zagrożeniach i podejmowanych działaniach;
- uzgodnienie z instytucjami wspierającymi zakresu i sposobu wykonania zadań;
- uzgodnienie standardów wyposażenia w sprzęt i oprogramowania informatycznego do wspomagania procesu zarządzania;
- opracowanie wspólnych raportów, analiz, programów i strategii postępowania;
- przygotowanie i realizacja porozumień i umów o współpracy;
- organizowanie i prowadzenie wspólnych szkoleń i ćwiczeń;
- zorganizowanie systemu punktów kontaktowych zapewniających sprawną wymianę informacji".

Powyższa lista uwzględnia nie tylko zadania z UZK, ale i UMOL. Co prawda w UMOL nie ma definicji fazy przygotowania, ale znajduje się w niej definicja gotowości; rozumiana jest ona jako „osiągnięty w wyniku podjętych uprzednio działań stan przygotowania zasobów ludzkich i środków materialnych, struktur, społeczności i organizacji do skutecznego szybkiego reagowania na klęskę lub katastrofę" (UMOL, art. 4, pkt 3). Wskazuje więc nie tyle, jakie zadanie (działania) należy podejmować w ramach przygotowania się na wypadek zaistnienia klęski lub katastrofy, ile raczej jaki efekt końcowy powinien zostać w ich wyniku osiągnięty.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

1.3.3. Faza trzecia – reagowanie

Faza reagowania jest często błędnie utożsamiana z całością zarządzania kryzysowego. Efektem takiego podejścia jest przekonanie, że realizacja zarządzania kryzysowego następuje dopiero po zaistnieniu zdarzenia nadzwyczajnego i sprowadza się do uruchomienia nowych procedur, odmiennych od stosowanych przy reagowaniu rutynowym. W rzeczywistości faza ta obejmuje następujące działania:

- monitorowanie, analizowanie i prognozowanie rozwoju zagrożeń,
- uruchomienie procedur reagowania kryzysowego,
- uruchomienie sił i środków,
- uruchomienie systemów ostrzegania i alarmowania,
- prowadzenie działań ratowniczych,
- informowanie ludności,
- zapewnienie opieki medycznej,
- ewakuacja prewencyjna ludności,
- stworzenie doraźnych warunków do przetrwania osób poszkodowanych,
- uruchomienie pomocy społecznej i psychologicznej,
- wsparcie działań przez organizacje społeczne i humanitarne,
- wsparcie działań przez Siły Zbrojne RP,
- wnioskowanie o ewentualną pomoc zagraniczną,
- zapewnienie sprawnego obiegu informacji.

1.3.4. Faza czwarta – odbudowa

Generalnie UZK odnosi się wyłącznie do usuwania skutków sytuacji kryzysowych oraz odtwarzania zasobów i IK (UZK, art. 2). Ponieważ sytuacja kryzysowa wymaga współistnienia sytuacji zagrożenia i jednoczesnej „nieadekwatności" w reagowaniu właściwych służb, nie można utożsamiać usuwania skutków sytuacji kryzysowej z usuwaniem skutków zagrożenia. Część kosztów związanych z usuwaniem skutków ponoszą sami obywatele, ewentualnie firmy ubezpieczeniowe. Na organach administracji rządowej i samorządowej spoczywa natomiast szereg obowiązków wynikających z innych ustaw. Najistotniejsze z nich to omówione już udzielanie pomocy społecznej. To zadanie często wymaga nadzwyczajnych działań organizacyjnych w tych przypadkach, gdy jego realizacja wiąże się z koniecznością zapewnienia minimalnych warunków bytowych ewakuowanej ludności lub skala udzielanej pomocy przekracza techniczne i finansowe możliwości gminy. Na takie przypadki plany zarządzania kryzysowego powinny przewidywać konieczność uzupełnienia osobowego służb socjalnych, wykorzystując do tego celu inne jednostki podległe gminie (choćby jednostki ochotniczej straży pożarnej), pododdziały bądź oddziały Sił Zbrojnych skierowane przez wojewodę i inne podobne rozwiązania. Innymi metodami wspierania fazy odbudowy jest

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

możliwość skorzystania z programów rządowych realizowanych poprzez Departament Ochrony Ludności i Zarządzania Kryzysowego MSWiA, jednak programy te nakierowane są głównie na odbudowę infrastruktury oraz obiektów będących w posiadaniu samorządu terytorialnego. Inną formą wspierania fazy odbudowy jest zastosowanie specjalnych (ułatwionych) procedur administracyjnych w sprawach dotyczących odbudowy obiektów uszkodzonych bądź zniszczonych na skutek działania żywiołu (DzU z 2016 r. poz. 1067) czy udzielanie kredytów.

Obowiązująca UZK nakazuje natomiast odtwarzanie zasobów zgromadzonych, a następnie zużytych w procesie reagowania kryzysowego. Drugim zadaniem wynikającym wprost z UZK jest obowiązek włączenia się organów zarządzania kryzysowego w odtworzenie IK. Zadanie to ma szczególne znaczenie, gdyż umożliwia administracji rządowej techniczne, organizacyjne i sprzętowe wsparcie posiadacza IK i to nawet wówczas, gdy posiadaczem jej jest podmiot niezwiązany z administracją.

1.4. Kierowanie i koordynacja działań w ramach zarządzania kryzysowego

1.4.1. Szczebel centralny

Przy ocenie faktycznych zdolności sprawowania funkcji kierowniczej niezbędnym jest rozpatrzenie możliwości realizacji następujących funkcji składowych:

- planowanie,
- organizowanie,
- przewodzenie,
- kontrolowanie (Lisiecki 2001).

Jednak z uwagi na bardzo ograniczone możliwości przejmowania kompetencji jednego organu przez inny w praktyce zarządzania kryzysowego najczęściej stosowanym określeniem obrazującym zakres oddziaływania na podległe sobie podmioty jest „koordynacja". Należy ją rozumieć jako zbiór czynności (decyzji) wykonywanych przez wszystkie szczeble kierownicze struktury, a szczególnie przez kierownictwo układu dla zapewnienia harmonijnego współdziałania pod-układów w celu osiągnięcia założonych celów całego układu (Gościński 1971).

W strukturze organów zarządzających sytuacjami kryzysowymi znalazła odzwierciedlenie generalna filozofia UZK zakładająca, że reagowanie w sytuacjach kryzysowych sprowadza się do wsparcia działań tego organu, którego siły i środki są nieadekwatne do zaistniałej sytuacji. Na szczeblu centralnym wyraźnie rozgraniczono dwa przypadki. W pierwszej kolejności zadania z obszaru zarządzania kryzysowego powinni realizować ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych (oczywiście tylko bezpośrednio zaangażowanych) (UZK, art. 12). Dopiero kiedy możliwości ministra (kierownika urzędu centralnego) będą nieadekwatne do sytuacji, zarządzanie powinna przejąć RM (UZK, art. 7 ust. 1). Narzędziem do realizacji zarządzania kryzysowego jest

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

plan zarządzania kryzysowego właściwego ministra (kierownika urzędu centralnego) i KPZK. W praktyce trudno sobie wyobrazić sytuację, w której zwalczanie będą zaangażowane wyłącznie służby podległe jednemu ministrowi. Stąd każdy z planów powinien zawierać między innymi elementy rutynowego wsparcia przez inne służby niezbędne w fazie reagowania. Podstawą uznania, że sytuacja wykracza poza możliwości właściwego ministra (ministra wiodącego w danej sytuacji) jest zatem stwierdzenie, że nie tylko wykracza ona poza obszar kompetencji organu wiodącego, ale również poza rozwiązania zawarte we właściwym planie zarządzania kryzysowego.

Drugim elementem wymagającym szczegółowego rozwiązania w planach zarządzania kryzysowego jest współpraca organów zarządzania kryzysowego szczebla centralnego z wojewodami oraz służbami, inspekcjami i strażami. W sytuacjach kryzysowych nie przewidziano zmiany podległości tych organów i w efekcie wojewoda podlega Prezesowi RM. Od zasady tej mogą być wyjątki, o ile wynikają one z poszczególnych ustaw branżowych (DzU z 2015 r. poz. 525, art. 8 ust. 1 i art. 9 ust. 1). Minister właściwy do usuwania danego zagrożenia może wykorzystać również podległość poszczególnych służb, inspekcji i straży wynikającą z ich pragmatyk. Zasady te ulegają zmianie po wprowadzeniu jednego ze stanów nadzwyczajnych. Przykładowo po wprowadzeniu stanu klęski żywiołowej na obszarze większym niż jedno województwo, wojewoda podlega nie Prezesowi RM, lecz właściwemu ministrowi. Minister ten w niektórych przypadkach może zawiesić uprawnienia wojewody i wyznaczyć pełnomocnika do kierowania działaniami (DzU z 2014 r. poz. 333, art. 11 ust. 3 i 4). Natomiast wojewodzie są podporządkowane organy i jednostki organizacyjne administracji rządowej i samorządu województwa działające na obszarze województwa oraz inne siły i środki wydzielone do jego dyspozycji i skierowane do wykonywania tych działań na obszarze województwa, w tym pododdziały i oddziały Sił Zbrojnych Rzeczypospolitej Polskiej (DzU z 2014 r. poz. 333, art. 8 i 9). Należy zauważyć, że uprawnienia te nie obejmują organów administracji publicznej. Jednocześnie nawet po wprowadzeniu stanu klęski żywiołowej, poza przypadkami ściśle opisanymi w tej ustawie, organy władzy publicznej działają w dotychczasowych strukturach organizacyjnych państwa i w ramach przysługujących im kompetencji (DzU z 2014 r. poz. 333, art. 7). Można więc wysnuć wniosek, że takie organy jak kierujący akcją ratowniczą czy policjant kierujący działaniami policyjnymi zachowują swoją niezależność.

Szczególną rolę UZK przewidziała dla ministra właściwego do spraw wewnętrznych. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów (UZK, art. 7 ust 2). Jednak jego uprawnień do sprawowania zarządzania kryzysowego nie należy traktować jako prawa do koordynowania działań poszczególnych ministrów, gdyż te zgodnie z Konstytucją są zastrzeżone wyłącznie dla Prezesa RM (Konstytucja RP, art. 148 i 149). Zakres działania ministra właściwego do spraw wewnętrznych zależy głównie

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

od postanowień KPZK. Plan podlega procedurze opiniowania przez RZZK i jest przedkładany RM na zasadach analogicznych jak wszystkie inne dokumenty rządowe. Stąd dokumentami wspólnymi dla wszystkich ministrów są takie elementy KPZK jak:

- tryb uruchamiania niezbędnych sił i środków,
- wykaz podmiotów uczestniczących w realizacji planowanych przedsięwzięć,
- procedury reagowania kryzysowego określające sposób postępowania w sytuacjach kryzysowych.

W tej sytuacji uprawnienia ministra właściwego do spraw wewnętrznych sprowadzają się głównie do uruchamiania wcześniej ustalonych procedur w imieniu Rady Ministrów, która pozostaje najwyższym organem zarządzania kryzysowego. Zakres, w jakim RM pełni tę funkcję, został w ustawie opisany w sposób nieprecyzyjny. Sformułowanie „na terytorium Rzeczypospolitej Polskiej" miało w swoim zamyśle podkreślać, że ustawa nie narusza ani praw innych państw, ani prawa międzynarodowego. Jest jednak interpretowane jako wręcz zakaz realizacji przez RM zarządzania kryzysowego poza terytorium RP. Warto zwrócić uwagę, że w myśl Konstytucji RP obywatelom RP przysługuje opieka podczas pobytu za granicą (Konstytucja RP, art. 36). Już ten fakt wskazuje na to, że w sytuacjach kryzysowych, które wystąpiły poza granicami RP, ale zagrażają polskim obywatelom, Rada Ministrów powinna odpowiednio zareagować. Jednak musi swoją reakcję dostosować do wymogów prawa międzynarodowego (Konwencja Wiedeńska z 1963 r.). Kontrowersyjne sformułowanie należy zatem interpretować następująco: w sytuacjach kryzysowych na terytorium RP RM sprawuje zarządzanie kryzysowe zgodnie z UZK; w przypadku sytuacji kryzysowych, jakie wystąpiły poza terytorium RP, ale mają wpływ na bezpieczeństwo jej obywateli lub jej żywotne interesy, RM sprawuje zarządzanie kryzysowe zgodnie z innymi rozwiązaniami prawnymi.

1.4.2. Szczebel wojewódzki

Na obszarze województwa organem sprawującym zarządzanie kryzysowe jest wojewoda (UZK, art. 14 ust. 1). W rzeczywistości wojewoda nie realizuje zadań samodzielnie ani wyłącznie na podstawie podległy sobie urząd. Podstawowym narzędziem do ich realizacji jest właściwy zapis w ustawie o wojewodzie. Zgodnie z nim wojewoda zapewnia współdziałanie wszystkich organów administracji rządowej i samorządowej działających w województwie i kieruje ich działalnością w zakresie zapobiegania zagrożeniu życia, zdrowia lub mienia oraz zagrożeniom środowiska, bezpieczeństwa państwa i utrzymania porządku publicznego, ochrony praw obywatelskich, a także zapobiegania klęskom żywiołowym i innym nadzwyczajnym zagrożeniom oraz zwalczania i usuwania ich skutków na zasadach określonych w odrębnych ustawach. Ponadto wykonuje i koordynuje zadania w zakresie obronności i bezpieczeństwa państwa oraz zarządzania kryzysowego

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

wynikające z odrębnych ustaw (DzU z 2015 r. poz. 525, art. 22 pkt. 2 i 4). W ramach realizacji swoich uprawnień wojewoda może wydawać polecenia obowiązujące wszystkie organy administracji rządowej działające w województwie, a w sytuacjach nadzwyczajnych obowiązujące również organy samorządu terytorialnego (DzU z 2015 r. poz. 525, art. 25 ust. 1). Sytuacjami nadzwyczajnymi są również sytuacje kryzysowe w rozumieniu UZK (DzU z 2015 r. poz. 525, art. 25 ust. 1a). Dodatkowo wojewoda na obszarze województwa określa zadania krajowego systemu ratowniczo-gaśniczego, koordynuje jego funkcjonowanie i kontroluje wykonywanie wynikających stąd zadań, a w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia lub środowiska kieruje tym systemem (DzU z 2017 r. poz. 736, art. 14 ust. 3). Wojewoda wykonuje te zadania przy pomocy wojewódzkiego zespołu zarządzania kryzysowego (DzU z 2017 r. poz. 736, art. 14 ust. 4).

Jak widać, kompetencje wojewody dotyczące reagowania w sytuacjach nadzwyczajnych, a tym samym w sytuacjach kryzysowych, są doprecyzowane w ustawach branżowych. Natomiast brakowało w nich odniesienia do pozostałych faz zarządzania kryzysowego. Zadania wojewody zawarte w UZK stanowią zatem wypełnienie tej luki i pozwalają wojewodzie na właściwe przygotowanie podległej sobie administracji do działań na wypadek wystąpienia sytuacji nadzwyczajnej, m.in. poprzez zintegrowane wielopodmiotowe planowanie, ciągłe doskonalenie umiejętności w ramach realizacji cyklu planowania oraz możliwość wsparcia działań organu wiodącego wydzielonymi pododdziałami i oddziałami Sił Zbrojnych RP. Podobnie jak w przypadku organów szczebla centralnego wojewoda również uzyskuje szczególne uprawnienia w przypadku wprowadzenia stanu klęski żywiołowej na obszarze większym niż jeden powiat. W takim przypadku wojewodzie podporządkowani są starostowie, organy i jednostki organizacyjne administracji rządowej i samorządu województwa działające na obszarze województwa oraz inne siły i środki wydzielone do jego dyspozycji i skierowane do wykonywania tych działań na obszarze województwa, w tym pododdziały i oddziały Sił Zbrojnych Rzeczypospolitej Polskiej (DzU z 2014 r. poz. 333, art. 11 ust. 2).

1.4.3. Szczebel samorządowy

Organem właściwym w sprawach zarządzania kryzysowego na obszarze powiatu jest starosta jako przewodniczący zarządu powiatu (UZK, art. 17 ust. 1)[3]. Jednak podobnie jak w przypadku wojewody zadania nałożone na starostę w ramach zarządzania kryzysowego bazują na jego kompetencjach wynikających z innych

[3] Rolę starosty należy rozpatrywać w trzech aspektach: jako organ samorządu powiatowego, jako organ administracji rządowej i wreszcie jako organ administracji publicznej, o ile ustawa upoważnia go do wydawania decyzji administracyjnych we własnym imieniu. Zaznaczenie, że starosta jest organem zarządzania kryzysowego w ramach pełnienia roli przewodniczącego zarządu powiatu, ma podkreślać, iż zadania przez niego realizowane są uzupełnieniem działań prowadzonych przez samorząd powiatowy. Brak tego dopisku mógłby sugerować, że starosta wypełnia te zadania wyłącznie w ramach administracji rządowej. To z kolei oznaczałoby, że takie działanie powinno być zlecone i opłacone przez wojewodę.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

ustaw. Podstawowymi są zadania własne samorządu powiatowego, przy których realizacji mogą pojawić się sytuacje kryzysowe. Poza zadaniami realizowanymi w ramach samorządu terytorialnego starosta jest organem administracji rządowej (DzU z 2015 r. poz. 525, art. 2 pkt. 5), a w konsekwencji zwierzchnikiem powiatowych służb, inspekcji i straży (DzU z 2016 r. poz. 814, art. 35 ust. 2 i 3). W ramach tych uprawnień m.in. uzgadnia wspólne działanie tych jednostek na obszarze powiatu, w sytuacjach szczególnych kieruje ich wspólnymi działaniami. Poszczególne ustawy branżowe uściślają zakres władztwa starosty w odniesieniu do służb powiatowych. Przykładowo w przypadku bezpośredniego zagrożenia bezpieczeństwa wspólnoty samorządowej, w szczególności życia lub zdrowia, starosta może wydać komendantowi powiatowemu (miejskiemu) PSP polecenie podjęcia działań w zakresie właściwości PSP zmierzających do usunięcia tego zagrożenia (DzU z 2017 r. poz. 1204, art. 14 ust. 3). Starosta do działań poza obszarem bezpośredniego kierowania akcją ratowniczą może wykorzystywać powiatowe jednostki krajowego systemu ratowniczo-gaśniczego. Powyższe wynika z postanowień ustawy o ochronie przeciwpożarowej, zgodnie z którą starosta na obszarze powiatu określa zadania krajowego systemu ratowniczo-gaśniczego, koordynuje jego funkcjonowanie i kontroluje wykonywanie wynikających stąd zadań, a w sytuacjach nadzwyczajnych zagrożeń życia, zdrowia lub środowiska kieruje tym systemem (DzU z 2017 r. poz. 736, art. 14 ust. 3). Analizując praktyczny wymiar zadań starosty, należy podkreślić jego rolę we właściwym planistycznym, organizacyjnym, sztabowym i szkoleniowym przygotowaniu wspólnych działań zarówno starostwa, jednostek organizacyjnych powiatu, jak i służb, inspekcji i straży powiatowych. Jednak w odniesieniu do fazy reagowania należy stwierdzić, że jego oddziaływanie na podmiot wiodący w zakresie likwidacji danego zagrożenia jest niewielkie. Poszczególne służby, inspekcje i straże zwalczają powstałe zagrożenie i jego skutki zgodnie z własnymi ustawami kompetencyjnymi. Natomiast ogromne znaczenie w tej fazie ma zapewnienie właściwego obiegu informacji i to zarówno w odniesieniu do służb reagowania (centrum zarządzania kryzysowego, system łączności, alarmowania i współdziałania (DzU z 2017 r. poz. 736, art. 21b pkt 4), jak i w odniesieniu do potencjalnie zagrożonych mieszkańców powiatu (monitorowanie zagrożeń oraz alarmowanie i ostrzeganie ludności (DzU z 2013 r. poz. 96).

Swoich zadań starosta nie wykonuje w oderwaniu od działań innych organów zarządzania kryzysowego. Związki z wojewodą, zarówno w sytuacjach kryzysowych, jak i po wprowadzeniu stanu klęski żywiołowej, zostały już omówione. Natomiast zależności pomiędzy starostą a wójtami (burmistrzami, prezydentami miast) nie są ustawowo uregulowane. Dotyczy to zarówno doraźnego reagowania, jak i sytuacji kryzysowych albo nadzwyczajnych. Powodem tego faktu jest konstytucyjna samodzielność jednostek samorządu terytorialnego, podlegająca ochronie sądowej (Konstytucja RP, art. 165 ust. 2). Narzędziem umożliwiającym współpracę starosty z wójtami (burmistrzami, prezydentami miast) jest możliwość wzajemnego udzielania sobie pomocy (DzU z 2016 r. poz. 814, art. 7a; DzU z 2016 r. poz. 446,

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

art. 10 ust. 2). Tą drogą samorządy mogą obniżyć koszty działań (zamiast przygotowywać np. po trzy tysiące miejsc ewakuacyjnych w każdej gminie, wystarczy przygotować ich tysiąc, a jednocześnie zapewnić sobie możliwość użycia miejsc przygotowanych w gminach sąsiednich). Dodatkowo mogą wprowadzić wspólny obieg informacji o zagrożeniach, posiadanych zapasach i podejmowanych działaniach. Wsparciem tych działań dla starosty może być obowiązek przygotowania zaleceń do gminnego planu zarządzania kryzysowego, prawo do zatwierdzania tego planu oraz prawo do żądania informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w UZK (UZK, art. 20a).

Zależności pomiędzy starostą a wójtami ulegają zmianie po wprowadzeniu stanu klęski żywiołowej. Jeśli stan taki wprowadzono na obszarze większym niż jedna gmina, wójtowie podlegają staroście. Starosta w razie niezdolności do kierowania lub niewłaściwego kierowania działaniami może zwrócić się do wojewody o zawieszenie uprawnień wójta i powołanie pełnomocnika. Decyzję taką może wydać wojewoda również z inicjatywy własnej (DzU z 2014 r. poz. 333, art. 9 ust. 4 i 5). Ponieważ UZK nie precyzuje, jak będzie wyglądał obieg informacji i zakres zadań realizowanych przez wójta podlegającego staroście, element ten powinien być włączony do gminnego i powiatowego planu zarządzania kryzysowego oraz podlegać wdrożeniu i weryfikacji w oparciu o cykl planowania.

Na terenie gminy organem właściwym w sprawach zarządzania kryzysowego jest wójt, burmistrz, prezydent miasta (UZK, art. 19 ust 1). Jednak w przeciwieństwie do pozostałych organów zarządzania kryzysowego wójt (burmistrz, prezydent miasta) nie realizuje zadań organu administracji rządowej. Jego kompetencje wynikają z ustawy o samorządzie gminnym. Zgodnie z nią wójt realizuje zadania przy pomocy urzędu gminy, a ponadto wykonuje uprawnienia zwierzchnika służbowego w stosunku do pracowników gminy i kierowników gminnych jednostek organizacyjnych. Dla tego szczebla UZK również przewidziała istnienie komórki urzędu właściwej w sprawach zarządzania kryzysowego. Wójt dodatkowo ma też do dyspozycji jednostki OSP. Wprawdzie są one stowarzyszeniami, ale realizują ustawowo zlecone zadania samorządu gminnego (Tabasz 1999), otrzymując na ten cel środki finansowe z budżetu gminy (DzU z 2017 r. poz. 736, art. 32 ust. 2). Wójtowi, podobnie jak staroście, w przypadku bezpośredniego zagrożenia bezpieczeństwa wspólnoty samorządowej, w szczególności życia lub zdrowia, przysługuje prawo wydawania kierownikom (komendantom) służb inspekcji i straży poleceń podjęcia działań zmierzających do usunięcia tego zagrożenia. Polecenie takie musi być zgodne z właściwością danej służby lub inspekcji.

Wójtowi przysługuje natomiast uprawnienie, którego nie posiada starosta, zaś wojewoda wyłącznie w bardzo ograniczonym zakresie. Tym uprawnieniem jest możliwość zarządzenia ewakuacji. Jednocześnie ustawa nie zawęża tych kompetencji ani do rodzaju zagrożenia, ani do jego wielkości. Jedyny wymóg, jaki musi spełnić organ wydający decyzję, to ocena, czy zagrożenie jest bezpośrednie i czy poza ewakuacją nie ma innego sposobu usunięcia zagrożenia (wyrok WSA

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

we Wrocławiu, III SA/Wr 504/12). W brzmieniu dosłownym: „Jeżeli w inny sposób nie można usunąć bezpośredniego niebezpieczeństwa dla życia ludzi lub dla mienia, wójt może zarządzić ewakuację z obszarów bezpośrednio zagrożonych" (DzU z 2016 r. poz. 446, art. 31b).

Istnieje poważna wątpliwość, czy to „zarządzenie ewakuacji" jest decyzją administracyjną kierowaną do konkretnego obywatela, czy raczej uruchomieniem wcześniej zaplanowanego procesu. Gdyby to była decyzja administracyjna, to na organie ją wydającym spoczywałby obowiązek jej wyegzekwowania. Formalne postępowanie w takiej sytuacji opisuje ustawa o postępowaniu egzekucyjnym w administracji (DzU z 2017 r. poz. 1201). Ustawa zarówno wskazuje organy uprawnione do egzekwowania omawianych decyzji, jak i przyznaje prawo do zastosowania przymusu bezpośredniego wobec osób uchylających się od jej wykonania (DzU z 2017 r. poz. 1201, art. 20 § 2 oraz rozdział 6). W przypadku powodzi, gdy nierzadko zachodzi konieczność ewakuacji kilku tysięcy osób jednocześnie, zastosowanie przymusu wymagałoby udziału ogromnej liczby policjantów i żołnierzy. Jest to zadanie wręcz niewykonalne. Przyjęcie, że „zarządzenie ewakuacji" oznacza jedynie uruchomienie procesu, sprawia, iż wójt jedynie stwarza warunki do ewakuacji (środki transportu, miejsce ewakuacji). Natomiast decyzję, czy z tej możliwości skorzystać, czy nie, podejmuje sam obywatel. Upoważnienie do zarządzenia ewakuacji przyznane wójtowi nie tylko wyróżnia go spośród innych organów zarządzania kryzysowego, ale nawet spośród organów administracji publicznej powoływanych doraźnie w celu zwalczania zagrożeń dla życia, zdrowia i mienia. Przykładowo strażak kierujący akcją ratowniczą może zarządzić ewakuację tylko z rejonu objętego działaniem ratowniczym, o ile istnieje zagrożenie dla życia i zdrowia, a jednocześnie istnieje groźba wybuchu paniki lub dalszy rozwój zdarzeń może doprowadzić do odcięcia drogi ewakuacyjnej (DzU z 1992 r. nr 54, poz. 259, § 1 ust. 1 pkt 1). W przeciwieństwie jednak do wójta sytuacja strażaka kierującego działaniem ratowniczym jest jednoznaczna. Decyzje przez niego wydawane są decyzjami administracyjnymi, może być im nadany rygor natychmiastowej wykonalności (co oznacza brak możliwości odwołania się od decyzji przed jej wykonaniem). W szczególnych przypadkach decyzja może być wydana ustnie, a potwierdzona pisemnie w terminie późniejszym (DzU z 1992 r. nr 54, poz. 259, § 1 ust. 2 oraz § 3 ust. 3). I choć możliwość zastosowania przymusu wobec osób chcących chronić własne domostwa jest wielce kontrowersyjna, to należy pamiętać o konsekwencjach jej niewyegzekwowania. W szczególności o tym, że skoro organ wydający decyzję jest zobowiązany do jej wyegzekwowania, to osoby poszkodowane lub ich spadkobiercy mogą dochodzić roszczeń z tytułu niedopełnienia przez niego ustawowych obowiązków[4].

Niezależnie czy ewakuacja będzie miała charakter dobrowolny, czy przymusowy, ani wójt, ani kierujący akcją ratowniczą nie są w stanie samodzielnie

[4] Zob. szerzej: http://www.tvn24.pl/krakow,50/stracili-domy-w-powodzi-pozwali-panstwo-zadaja-17-milionow-zlotych,407416.html

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

przeprowadzić takiej operacji na większym obszarze. Aby się powiodła, niezbędny będzie udział co najmniej policji, a w poważniejszych przypadkach również Sił Zbrojnych. Stąd zasady przeprowadzenia ewakuacji, w tym zakres wsparcia wójta przez siły policji i wojska, powinny zostać określone w zaleceniach do gminnych planów zarządzania kryzysowego wydawanych przez starostę.

Mimo że celem ustawy jest udzielanie wsparcia tej służbie czy organowi, którego możliwości są nieadekwatne do zagrożenia, to najniższy szczebel zarządzania kryzysowego nie jest jedynie beneficjentem udzielanej pomocy. W rzeczywistości rola wójta, a szerzej samorządu gminnego, jest nieporównywalnie większa. Szczególny charakter zadań realizowanych na tym szczeblu wynika z faktu, że zadaniem własnym samorządu gminnego jest udzielanie pomocy społecznej. Pomoc ta udzielana jest m.in. w przypadku zdarzenia losowego oraz klęski żywiołowej i ekologicznej (DzU z 2016 r. poz. 930, art. 7 pkt. 14 i 15). W jej zakres wchodzą m.in.:

- udzielanie schronienia, zapewnienie posiłku oraz niezbędnego ubrania osobom tego pozbawionym,
- przyznawanie i wypłacanie zasiłków okresowych,
- przyznawanie i wypłacanie zasiłków celowych,
- przyznawanie i wypłacanie zasiłków celowych na pokrycie wydatków powstałych w wyniku zdarzenia losowego (DzU z 2016 r. poz. 930, art. 17 ust. 1) (przy czym wypłacanie zasiłków celowych na pokrycie wydatków związanych z klęską żywiołową lub ekologiczną jest zadaniem zleconym z zakresu administracji rządowej realizowanym przez gminę, zatem podlega refundacji z budżetu państwa).

Faktycznie zatem, niezależnie od tego, który organ administracji publicznej podejmie decyzję o ewakuacji, obowiązek zapewnienia osobom ewakuowanym minimalnych niezbędnych warunków do życia pozostaje zadaniem samorządu gminnego. Możliwości wsparcia tych działań ze strony wyższych szczebli zarządzania kryzysowego są mocno ograniczone. W praktyce sprowadzają się one do wsparcia finansowego poprzez dotacje udzielane za pośrednictwem budżetu wojewody oraz w trybie stosowanym przez Departament Ochrony Ludności i Zarządzania Kryzysowego MSWiA[5]. Podstawowym sposobem uniknięcia przez poszczególne gminy poważnych perturbacji w przypadku konieczności tymczasowego zakwaterowania dużej grupy ludzi wydaje się być tryb wspólnej realizacji zadań przy udziale starosty jako koordynatora.

1.5. Struktura organizacyjna zarządzania kryzysowego

1.5.1. Szczebel centralny

Na każdym szczeblu ustawa przewiduje funkcjonowanie kilku zasadniczych elementów systemu zarządzania kryzysowego. Są nimi:

[5] Zob. https://mswia.gov.pl/pl/bezpieczenstwo/usuwanie-skutkow-klesk [dostęp 19.12.2017].

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

- decydent,
- doraźnie działający zespół doradczo-sztabowy,
- komórka obsługująca zarówno decydenta, jak i posiedzenia zespołu doradczego,
- stanowisko odpowiedzialne za monitorowanie sytuacji i obieg informacji.

Na szczeblu centralnym mamy do czynienia z dwoma zasadniczymi organami zarządzania kryzysowego. Są nimi minister odpowiedzialny za dany dział administracji rządowej (UZK, art. 12) (ewentualnie inny organ centralny) oraz RM. Zgodnie z definicją sytuacji kryzysowej sprawowanie zarządzania kryzysowego przez RM jest związane z wystąpieniem sytuacji kryzysowej przy zdarzeniu obsługiwanym przez ministra (kierownika urzędu centralnego). Dla oceny, czy taka sytuacja wystąpiła, konieczne jest posiadanie informacji o skali zagrożenia, rodzaju i wielkości zaangażowanych sił oraz spodziewanej eskalacji zdarzenia. Większość tych danych można pozyskać albo poprzez międzynarodowy i krajowy monitoring sytuacji realizowany w ramach danej branży (inspekcja sanitarna, PSP itp.), albo poprzez wojewodów. Dla bieżącego zbierania niezbędnych danych UZK przewiduje powołanie odpowiednich centrów zarządzania kryzysowego. Do ich powołania zostali zobowiązani ministrowie i centralne organy administracji rządowej, do zakresu działania których należą sprawy związane z zapewnieniem bezpieczeństwa narodowego, w tym ochrony ludności lub gospodarczych podstaw bezpieczeństwa państwa. Szczegółową listę tych organów określa rozporządzenie RM (DzU z 2009 r. nr 226, poz. 1810). Zgodnie z nim centra mają tworzyć:

- minister obrony narodowej,
- minister sprawiedliwości,
- minister właściwy do spraw zagranicznych,
- minister właściwy do spraw rolnictwa,
- minister właściwy do spraw środowiska,
- minister właściwy do spraw zdrowia.

Do tej listy należy dodać ministra właściwego do spraw wewnętrznych, gdyż funkcję jego centrum zarządzania kryzysowego realizuje RCB. Natomiast, pomimo wskazania ustawowego, na liście nie znaleźli się tak istotni dla gospodarczych podstaw bezpieczeństwa państwa ministrowie jak minister właściwy do spraw gospodarki czy infrastruktury. Rozporządzenie szczegółowo omawia zasady organizacji, wyposażenie i funkcje realizowane przez tworzone centra. Najistotniejszym elementem rozporządzenia jest określenie zasad przekazywania informacji pomiędzy poszczególnymi centrami. Wprowadzono obowiązek przekazywania do RCB raportów sytuacyjnych raz dziennie, a po wprowadzeniu stanu nadzwyczajnego i w sytuacjach kryzysowych – zgodnie z zapotrzebowaniem. Co jest szczególnie ważne, w sytuacjach kryzysowych wiodącą rolę w zakresie pozyskiwania informacji, ich analizy i dystrybucji pełni centrum zarządzania kryzysowego obsługujące

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

organ, we właściwości którego pozostaje rodzaj zaistniałej sytuacji kryzysowej. Zapis ten pozwala uniknąć sytuacji, gdy różne centra zbierają i analizują dane, w wyniku czego podejmują różne, wzajemnie niespójne działania.

Dla pozostałych ministrów i organów centralnych funkcję centrum zarządzania kryzysowego będzie realizować RCB, przynajmniej do momentu uruchomienia przez nich własnego centrum zbierającego informacje. Przy takiej konstrukcji obiegu informacji mogą pojawić się problemy związane z niespójnością danych. Z jednej bowiem strony działają branżowe systemy monitorowania sytuacji, a z drugiej stanowiska obsługujące organy administracji ogólnej. Weryfikacja, czy właściwy organ otrzymał niezbędną informację oraz czy informacje zbierane dwutorowo pozostają ze sobą spójne, jest jednym z istotnych zadań RCB. Drugim problemem związanym z takim obiegiem danych jest konieczność zapewnienia spójnej polityki informacyjnej. To zadanie, ustawowo przypisane RCB, w praktyce oznacza, że w przypadku zdarzeń przypisanych jednemu z ministrów, RCB powinno dostarczać mu takich danych, by mógł samodzielnie prowadzić politykę informowania społeczeństwa nawet wówczas, gdy część zadań realizują organy, służby i podmioty mu niepodlegające.

Poza stanowiskami kierowania, do obsługi organu niezbędny jest zespół sztabowy konieczny do merytorycznej oceny zebranych danych i przygotowania najważniejszych decyzji. W tym przypadku ustawa nakazuje powołanie własnych zespołów zarządzania kryzysowego wszystkim ministrom kierującym działem administracji rządowej oraz kierownikom urzędów centralnych, do zakresów których należą sprawy zarządzania kryzysowego (UZK, art. 12 ust. 2b). W UZK pozostawiono dużą swobodę co do składu tych zespołów, szczegółowo natomiast określono zadania przez nie realizowane. Warto zwrócić uwagę, że nie są to wyłącznie zadania realizowane w fazie reagowania. Zadaniem zespołów jest bowiem m.in. dokonywanie okresowej oceny zagrożeń na potrzeby raportu o zagrożeniach bezpieczeństwa narodowego oraz opiniowanie projektów planów zarządzania kryzysowego.

Niezależnie od zespołów podlegających poszczególnym ministrom i kierownikom urzędów centralnych funkcjonuje RZZK obsługiwany przez RCB (UZK art. 8). W tym przypadku ustawodawca określił skład zespołu, wskazując jednocześnie jego członków stałych (ich obecność lub obecność ich uprawnionych przedstawicieli jest na posiedzeniu obowiązkowa) oraz członków, którzy biorą udział w posiedzeniu w zależności od potrzeb. Specjalny tryb pozostawiono dla przedstawiciela prezydenta. W tym przypadku prezydent sam decyduje o udziale swojego przedstawiciela w posiedzeniu RZZK, któremu przysługują takie same uprawnienia jak innym członkom RZZK. Szczegółową organizację i tryb pracy zespołu reguluje odpowiednie zarządzenie Prezesa RM (MP z 2014 r. poz. 926). Zgodnie z nim RZZK może podejmować decyzje na zwoływanych posiedzeniach lub w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy). Ponadto w celu realizacji zadań zespołu jego przewodniczący, z własnej inicjatywy

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

lub na wniosek sekretarza albo członka zespołu, może tworzyć zespoły robocze złożone z organów i osób, które wchodzą w skład RZZK. Przewodniczący zespołu wyznacza osobę kierującą zespołem roboczym oraz określa jego skład, zadania, tryb i miejsce pracy. To rozwiązanie pozwala na uruchomienie wspólnego dla członków RM sztabu pracującego w sposób ciągły (konieczność takiego rozwiązania jest jednym z wniosków wyciągniętych z organizacji turnieju EURO 2012 oraz po organizacji Światowych Dni Młodzieży 2016).

1.5.2. Szczebel wojewódzki

Dla szczebla wojewódzkiego UZK przewidziała funkcjonowanie zarówno komórki urzędu wojewódzkiego zajmującej się bieżącym realizowaniem zadań z zakresu planowania cywilnego (UZK, art. 16 ust. 1), stanowiska obsługującego obieg informacji (centrum zarządzania kryzysowego) (UZK, art. 16 ust. 3), jak i zespół doradczo-sztabowy (wojewódzki zespół zarządzania kryzysowego, WZZK) (UZK, art. 14). Specyfika zadań realizowanych na tym szczeblu sprowadza się do koordynacji i harmonizacji zadań przygotowywanych i realizowanych przez inne organy administracji publicznej, w tym takie, które nie podlegają wprost wojewodzie. Dodatkowo wojewoda ustawowo posiada również zadania własne, których z kolei nie może realizować bez czynnego zaangażowania innych organów i podmiotów[6]. Na tym szczeblu realizowane jest również jedno z najważniejszych zadań planowania cywilnego, sprowadzające się do zapewnienia spójności planów zarządzania kryzysowego z planami sporządzanymi przez inne organy na bazie ustaw „branżowych". W sumie komórka organizacyjna urzędu wojewódzkiego właściwa w sprawach zarządzania kryzysowego, realizując powyższe zadanie, powinna dokonać porównania wszystkich planów pod kątem ich spójności. Drugim celem tego porównania powinno być zdefiniowanie tych sytuacji, gdy możliwości działania służby właściwej do zwalczania danego zagrożenia zostaną wyczerpane, a zatem zaistnieją przesłanki do uznania sytuacji za kryzysową. Wiąże się z tym konieczność uruchomienia wsparcia dla organu wiodącego, w tym skorzystanie z pomocy ze strony Sił Zbrojnych. Ponadto omawiana komórka ma szczególne zadanie, które nie występuje na innych poziomach administracji. Tym zadaniem jest dostarczanie niezbędnych informacji dotyczących aktualnego stanu bezpieczeństwa dla wojewódzkiego zespołu zarządzania kryzysowego, zespołu zarządzania kryzysowego działającego w urzędzie obsługującym ministra właściwego do spraw wewnętrznych oraz RCB. Ocena stanu bezpieczeństwa to nie tylko rejestr zdarzeń aktualnych i przewidywalnych oparty na bieżącym monitorowaniu zagrożeń. To również ocena spodziewanych skutków zdarzeń i to zarówno w perspektywie krótko-, jak i długoterminowej.

[6] Przykładem takiej sytuacji są postanowienia art. 84, 86 i 89 ustawy – Prawo atomowe (DzU z 2017 r. poz. 576).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Bieżącym monitorowaniem zagrożeń w celu wykrycia symptomów sytuacji kryzysowej zgodnie z UZK zajmują się centra zarządzania kryzysowego powoływane w ramach komórek zarządzania kryzysowego. Ponieważ znaczna część zagrożeń dzięki branżowym systemom monitorowania wykrywana jest przez służby, inspekcje i straże, dla właściwego realizowania swoich zadań centrum zarządzania kryzysowego musi na bieżąco współpracować ze wszystkimi tymi podmiotami. Z uwagi na „pionowy" przepływ informacji w ramach poszczególnych służb, inspekcji i straży, centrum zarządzania kryzysowego realizuje też zadania związane z koordynowaniem przekazywania informacji w układzie terytorialnym. Narzędziem niezbędnym do realizacji powyższego zadania są postanowienia wojewódzkiego planu zarządzania kryzysowego, gdzie w ramach siatki bezpieczeństwa określone mają być służby, które powinny być powiadamiane o danym rodzaju zdarzenia. Obieg informacji o potencjalnych lub faktycznych zagrożeniach może też wynikać z innych ustaw. Na przykład organizator imprezy masowej jest zobowiązany z odpowiednim wyprzedzeniem informować właściwe gminne (miejskie) centrum zarządzania kryzysowego, a jeśli w danej gminie nie zostało ono utworzone – wojewódzkie centrum zarządzania kryzysowego. Centrum, które otrzymało takie zgłoszenie, ma obowiązek powiadomić inne instytucje wymienione wprost w ustawie (DzU z 2015 r. poz. 1485 ze zm., art. 22 ust. 1 i 2 w powiązaniu z art. 8).

Organem sztabowo-doradczym wojewody w sprawach zarządzania kryzysowego jest WZZK. Z uwagi na konieczność wspólnego i spójnego realizowania cyklu planowania przez wszystkie służby, inspekcje i straże przewidywane do działań w sytuacjach kryzysowych, niezbędnym warunkiem jest ich aktywny udział w pracach WZZK. Drugim istotnym zadaniem WZZK jest przygotowywanie propozycji działań w sytuacjach kryzysowych. Nie dotyczy to tylko propozycji zapisów w planie zarządzania kryzysowego. Najlepszy nawet plan nie jest w stanie przewidzieć wszystkich sytuacji, jakie mogą wystąpić w rzeczywistości. Dlatego przygotowanie propozycji działań może być formą szybkiej adaptacji planu do warunków, jakie realnie wystąpiły. Do zadań zespołu należy również ustalenie formy informowania społeczeństwa o istniejących lub przewidywanych zagrożeniach oraz skutkach, jakie mogą one wywołać.

Problem informowania jest niezwykle delikatny i złożony. Z jednej strony brak należytej informacji może przyczynić się do powstania plotek obniżających poziom poczucia bezpieczeństwa. Z kolei informacja podana w sposób niewłaściwy może wywołać panikę. Optymalna informacja powinna nie tylko powiadamiać o zaistniałej sytuacji i możliwości jej eskalacji, ale podawać również podstawowe sposoby postępowania przez osoby zagrożone oraz wskazywać, jakie działania władze już podjęły i zamierzają podjąć w celu likwidacji zagrożenia.

Ostatnim zadaniem ustawowym WZZK jest opiniowanie wojewódzkiego planu zarządzania kryzysowego. W efekcie kierownicy jednostek organizacyjnych planowanych do wykorzystania przy realizacji przedsięwzięć określonych

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

w planie mają dwukrotny wpływ na postanowienia planu. Po pierwsze uzgadniają plan w części ich dotyczącej, a po drugie jako członkowie WZZK – opiniują całość dokumentu. Wprowadzenie takiego trybu ma na celu wyeliminowanie przypadków, gdy wykonawca nie jest w stanie zrealizować postawionych zadań. Jednocześnie mając wpływ na całość dokumentu, wykonawca zna nie tylko zakres wsparcia, jaki mogą udzielić mu inne służby, ale posiada wiedzę na temat rodzaju i skali przewidywanych działań na terenie województwa oraz możliwości techniczne, organizacyjne i zasoby pozostałych uczestników działań.

1.5.3. Szczebel samorządowy

Struktura organizacyjna tworzona na potrzeby zarządzania kryzysowego w powiecie nie odbiega od rozwiązań przyjętych dla szczebla wojewódzkiego. I tak organem sztabowo-doradczym starosty jest powiatowy zespół zarządzania kryzysowego (UZK art. 17 ust. 4), zaś stanowiskiem zapewniającym obieg informacji powiatowe centrum zarządzania kryzysowego (UZK art. 18 ust 1–3). Zadania zespołu powiatowego są identyczne z zadaniami zespołu wojewódzkiego. Zdecydowanie inny jest natomiast sposób realizacji zadań starosty jako organu zarządzania kryzysowego. W tym przypadku nie ma obowiązku tworzenia komórki właściwej do spraw zarządzania kryzysowego. Wszystkie swoje zadania starosta może wykonywać przy pomocy powiatowej administracji zespolonej. Administrację tę stanowią:

- starostwo powiatowe,
- powiatowy urząd pracy, będący jednostką organizacyjną powiatu,
- jednostki organizacyjne stanowiące aparat pomocniczy kierowników powiatowych służb, inspekcji i straży (DzU z 2016 r. poz. 814, art. 33b).

W rezultacie takiego zapisu starosta ma wiele możliwości do wyboru, począwszy od powołania odpowiedniej komórki organizacyjnej w urzędzie powiatowym, poprzez całościowe bądź częściowe przekazanie swoich zadań do realizacji poszczególnym jednostkom stanowiącym aparat pomocniczy kierowników powiatowych służb, inspekcji i straży (należy zwrócić uwagę, że zadania są realizowane nie poprzez poszczególnych kierowników, lecz poprzez ich aparat pomocniczy. Jednocześnie UZK znacząco zwiększyła zakres odpowiedzialności starosty za funkcjonowanie centrum. W szczególności starosta ponosi pełną, ustawową odpowiedzialność za sposób całodobowego alarmowania członków zespołu zarządzania kryzysowego oraz sposób zapewnienia całodobowego obiegu informacji w sytuacjach kryzysowych.

Jedną z możliwości zapewnienia niezbędnego obiegu informacji jest stworzenie wspólnego centrum zarządzania kryzysowego działającego zarówno na potrzeby miasta na prawach powiatu, jak i powiatu ziemskiego. Warunkiem realizacji tego wariantu jest zawarcie porozumienia pomiędzy obiema jednostkami samorządu terytorialnego o wspólnej realizacji zadania ustawowego. Powołanie wspólnej jednostki nie zmienia pozostałych obowiązków ciążących na staroście, nadal zatem obowiązuje wymóg powołania odrębnych zespołów zarządzania kryzysowego. Oba organy zarządzania

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

kryzysowego muszą też odrębnie podjąć decyzję, czy realizują swoje zadania na bazie komórki powołanej w urzędzie ich obsługującym, czy decydują się na ich powierzenie urzędowi obsługującemu jedną z powiatowych służb, inspekcji i straży.

Specyfika funkcji realizowanych w ramach zarządzania kryzysowego przez szczebel gminny została już omówiona. Innym elementem różnicującym ten poziom jest odmienność organizacyjna. O ile na szczeblach wyższych struktura została narzucona ustawowo, to w przypadku gminy elementy wymagane to powołanie komórki urzędu właściwej w sprawach zarządzania kryzysowego (UZK, art. 19 ust. 3) oraz zorganizowanie zespołu zarządzania kryzysowego (art. 19 ust. 4). Natomiast decyzji wójta (odpowiednio burmistrza, prezydenta miasta) pozostawiono tak istotny element jak powołanie centrum zarządzania kryzysowego (UZK, art. 20 ust. 2). Podstawowe przesłanki tej regulacji to ograniczone możliwości finansowe wielu gmin w kraju oraz fakt, że gmina realizuje w ramach zarządzania kryzysowego nieomal wyłącznie własne zadania ustawowe. Dlatego sama powinna oceniać, jakimi środkami technicznymi jest w stanie je wykonywać. Podobnie jak w przypadku szczebla powiatowego, UZK dopuszcza możliwość powoływania wspólnych centrów obsługujących kilka samorządów. Jednak dotyczy to jedynie tych miejscowości, które są siedzibami jednocześnie dwóch lub więcej samorządów gminnych. Można zatem tworzyć wspólne centrum zarządzania kryzysowego, jeśli w danej miejscowości siedzibę ma jednocześnie samorząd miejski i wiejski.

Dowolność powoływania centrów zarządzania kryzysowego nie oznacza, że realizacja zadań wykonywanych przez centra też jest dobrowolna. Zgodnie z UZK zadania muszą być realizowane nadal, natomiast wójt ma obowiązek zapewnić ich realizację w sposób, jaki uzna za najwłaściwszy. Jednocześnie ponosi całkowitą odpowiedzialność za skuteczność przyjętego rozwiązania.

1.6. Współdziałanie organów zarządzania kryzysowego

W każdej instytucji i w każdym procesie decyzyjnym kluczową kwestią pozostaje organizacja systemu obiegu informacji, obiegu wielokierunkowego. Chodzi bowiem nie tylko o proste zależności pomiędzy podmiotami nadrzędnymi i podległymi, ale również o powiązania poziome, tj. pomiędzy podmiotami tego samego szczebla organizacyjnego czy decyzyjnego.

Nie ulega wątpliwości, że niższe szczeble zarządzania kryzysowego winny zarówno informować szczeble wyższe o swych działaniach, jak i być przez nie informowane w zakresie niezbędnym dla właściwego realizowania swych kompetencji ustawowych. Powinny również, szczególnie w trakcie sytuacji kryzysowej, informować się nawzajem o rozwoju sytuacji na równoległym szczeblu decyzyjnym, w tym przypadku na równoległym szczeblu podziału terytorialnego (sąsiednie gminy, powiaty, województwa). Należy jednak pamiętać, że nie w każdej sytuacji obowiązuje zasada powszechnego dostępu do informacji. Na przykład w zakresie obiegu informacji niejawnych obowiązuje reguła koniecznej wiedzy nazywana „*need to know*".

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Powyższymi ograniczeniami objęte są kwestie związane z ochroną IK oraz zagadnienia związane z realizacją zadań z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym. Obiegu informacji w systemie zarządzania kryzysowego nie należy mylnie utożsamiać z obiegiem decyzji w tym systemie oraz ze szczeblami odpowiedzialności za działania i decyzje. Organy zarządzania kryzysowego obowiązuje zasada subsydiarności (UZK, art. 21). Oznacza ona w tym przypadku, że dla ustawodawcy rzeczą kluczową w systemie jest szybkość reakcji, której podporządkowano inne, formalne uwarunkowania decyzyjne. Nawet więc jeśli pierwszy informację o zdarzeniu powziął szczebel „niewłaściwy" ze względu na skalę, miejsce zdarzenia lub swoje kompetencje, to zobowiązany jest do podjęcia stosownych, leżących w jego możliwościach działań. Ma to zapobiec znanej z administracji technice odsuwania od siebie odpowiedzialności pod pozorem rzekomych uwarunkowań formalnoprawnych.

Drugą kluczową kwestią dla ustawodawcy jest szybkość obiegu informacji o zdarzeniu. Pierwszym reagującym może być szczebel nieposiadający właściwych kompetencji do poradzenia sobie z sytuacją (np. zagrożenie o skali wojewódzkiej zauważono najpierw w gminie) lub odwrotnie – posiadający nadmierne kompetencje (np. pierwszy informacje powziął szczebel powiatowy, a sytuacja dotyczy jednej gminy). Dlatego szybkość przekazania informacji o zdarzeniu do szczebli niższego i wyższego decyduje o tym, kiedy działania będą podjęte przez organ właściwy do sytuacji. Ponadto informowane organy powinny natychmiast rozpocząć monitorowanie sytuacji i przygotowywać się do wsparcia organu, który jako pierwszy podjął reakcję.

Tak więc niezwłocznie po zaistniałym zdarzeniu szczeble wyższy i niższy powinny dysponować nie tylko informacją o zdarzeniu przekazaną przez pierwszy szczebel reakcji, ale również sporządzoną przez niego oceną sytuacji oraz planem zamierzonych działań. Na ocenę sytuacji będzie składać się oszacowanie skali zagrożenia, możliwych przyczyn i prawdopodobnego rozwoju sytuacji. Z tym ostatnim łączy się informacja o zamierzonych działaniach, których skala i waga musi być adekwatna do stopnia zagrożenia i do możliwego jego rozwoju. Taka informacja, oczywiście obok innych źródeł wiedzy (m.in. informacji medialnych i dodatkowego doprecyzowania w bezpośrednim kontakcie za pomocą dostępnych środków łączności), stanowi podstawę do podjęcia decyzji przez szczebel wyższy w sprawie ewentualnego włączenia się do działań[7].

[7] Mimo że zależności i obieg informacji pomiędzy organami zarządzania kryzysowego są logiczne i osadzone w prawie, jak dowodzą liczne analizy wykonywane w RCB, wzajemne informowanie się o zagrożeniach i podejmowanych działaniach często zawodzi. Przykładowo w czasie nawałnic, jakie miały miejsce w Polsce w dniach 10–12.08.2017, część gmin nie dowiedziała się o zagrożeniu, gdyż dyżurni powiatowych centrów zarządzania kryzysowego pełnili dyżur w domu pod telefonem, bez możliwości obsługi systemów monitorowania i poczty. Z kolei po zdarzeniu, ze względu na awarie sieci telefonicznych, zarówno stacjonarnych jak i komórkowych, wyższe szczeble administracji nie zostały poinformowane o sytuacji kryzysowej (zob. Załącznik do sprawozdania z prac międzyresortowego zespołu do spraw oceny funkcjonowania ratownictwa i zarządzania kryzysowego przyjętego przez Radę Ministrów 17.10.2017 r.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Szczególnym przypadkiem subsydiarności opisanym w UZK są zależności pomiędzy najwyższymi szczeblami systemu zarządzania kryzysowego. W myśl ustawy w sytuacjach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych (UZK, art. 7 ust. 2). Pojawia się tu problem, w jaki sposób i w jakim zakresie jeden z członków Rady Ministrów miałby działać w jej zastępstwie lub w jej imieniu. Aby odpowiedzieć na ten dylemat, należy zwrócić uwagę, że Rada Ministrów, realizując zadania nałożone UZK, m.in. przyjmuje szereg dokumentów, wśród których znajduje się Krajowy Plan Zarządzania Kryzysowego. W dokumencie tym są zawarte m.in. procedury reagowania kryzysowego oraz standardowe procedury operacyjne z zakresu zarządzania kryzysowego. Procedury wskazują, kto i jakie działania ma podejmować w zależności od rodzaju zdarzenia. W praktyce minister właściwy do spraw wewnętrznych uruchamia jedynie procedury przyjęte wcześniej przez RM jako obowiązujące wszystkich jej członków. Jest to zatem sytuacja, w której jeden z członków RM przejmuje jej kompetencje. Jednocześnie sprawujący w sytuacjach niecierpiących zwłoki zarządzanie kryzysowe minister właściwy do spraw wewnętrznych musi o swych działaniach zawiadomić niezwłocznie Prezesa RM. Jednak ewentualne działania premiera w tym zakresie, korygujące działania szefa MSW, będą wynikać z innych ustaw niż UZK, która stanowi jedynie, że decyzje podjęte przez ministra właściwego do spraw wewnętrznych podlegają rozpatrzeniu na najbliższym posiedzeniu RM. Te inne ustawy to przede wszystkim Konstytucja RP, zgodnie z którą Prezes RM koordynuje i kontroluje pracę członków RM .

Ponieważ proces zarządzania kryzysowego obejmuje wszystkie cztery fazy działań, obieg informacji nie może ograniczać się jedynie do fazy reagowania. Ustawodawca wskazał, iż kolejne szczeble decyzyjne muszą być zapoznane z planami zarządzania kryzysowego niższych szczebli, analizami zagrożeń i ryzyka, wreszcie planami odbudowy. Ponadto wnioski wynikające z raportu o zagrożeniach bezpieczeństwa narodowego muszą być przekazywane niższym szczeblom terytorialnym i resortowym w celu uwzględnienia w opracowywanych przez nie planach zarządzania kryzysowego .

Powyższa zasada pełnego informowania jest jednak ograniczona dostępem do informacji niejawnych. W przypadku wykazu obiektów IK obieg informacji został ograniczony do szczebla ministrów, kierowników urzędów centralnych oraz wojewodów, którym dyrektor RCB przekazuje właściwe wyciągi z wykazu IK. Podobnie właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń IK są jedynie informowani o ujęciu w wykazie, bez przekazywania pełnych wyciągów. Z kolei samorządy szczebla powiatowego i gminnego są jedynie selektywnie, w niezbędnym zakresie wynikającym z potrzeb prawidłowego funkcjonowania systemu zarządzania kryzysowego, i nieobligatoryjnie informowani przez właściwego wojewodę (z zachowaniem przepisów ustawy o ochronie

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

informacji niejawnych) o istnieniu na ich terenie działania obiektów, urządzeń i systemów IK.

Obieg informacji na szczeblu centralnym zapewnia RCB, szczególnie w zakresie organów wchodzących w skład RZZK. Zgodnie z UZK to właśnie za pośrednictwem RCB ministrowie i szefowie urzędów centralnych uzyskują informacje „o potencjalnych zagrożeniach oraz działaniach podjętych przez właściwe organy", także w zakresie wymiany informacji z podmiotami zagranicznymi. Aby wykonać to zadanie, RCB rozwija narzędzie informatyczne pod nazwą Centralnej Aplikacji Raportującej (CAR). Stale rozbudowywana aplikacja pozwala kolejnym uczestnikom systemu zarządzania kryzysowego na składanie w formie elektronicznej raportów doraźnych o występujących zagrożeniach, dobowych raportów o charakterze statystyczno-analitycznym oraz raportów sytuacyjnych o prowadzonych działaniach (w szczególności o działaniach długotrwałych).

1.7. Planowanie w zarządzaniu kryzysowym

1.7.1. Cykl planowania

Planowanie działań to nie tylko samo sporządzenie dokumentu ustalającego, kto, co, jak i współdziałając z kim wykona. Tworzony plan nie może też pomijać dokumentów już wykonanych. Z jednej strony ich nieuwzględnianie doprowadza do sytuacji, gdy te same siły i środki są ujęte z podobnymi lub różnymi zadaniami w różnych dokumentach. Ponadto ciągłe zwiększanie ilości dokumentów w pewnym momencie uniemożliwia ich prawidłowe wykorzystanie (Skomra 2004). Dlatego w UZK znalazło się omawiane już wcześniej stwierdzenie, że jednym z elementów planowania cywilnego jest „zapewnienie spójności między planami zarządzania kryzysowego a innymi planami sporządzanymi w tym zakresie przez właściwe organy administracji publicznej, których obowiązek wykonania wynika z odrębnych przepisów" (UZK, art. 4 ust. 1 pkt 6). Tym samym podstawą sporządzenia poszczególnych planów zarządzania kryzysowego są plany już przygotowane przez poszczególne służby, inspekcje i straże na bazie ich ustaw branżowych. Jest to zgodne z ogólną filozofią UZK, która zakłada wspieranie tego organu lub podmiotu, którego siły i środki okazały się nieadekwatne do zagrożenia.

Poza uwzględnieniem dokumentów już istniejących prawidłowe planowanie powinno być oparte na cyklu działania zorganizowanego. Według tradycyjnej koncepcji H. Le Châteliera warunkiem funkcjonowania jakiejkolwiek struktury jest właściwe organizowanie działań w cyklu, który obejmuje pięć kolejno po sobie następujących etapów:

- wybór celu, jaki chce się osiągnąć;
- zbadanie warunków i środków, które trzeba zastosować, aby osiągnąć zamierzony cel;

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

- przygotowanie warunków i środków uznanych za potrzebne;
- wykonanie stosownie do powziętego planu;
- kontrolę otrzymanych wyników (Lisiecki 2001, s. 12).

W odniesieniu do systemu zarządzania kryzysowego odpowiednikiem tego podejścia jest cykl planowania cywilnego (UZK, art. 3 pkt 7), który składa się z następujących etapów:

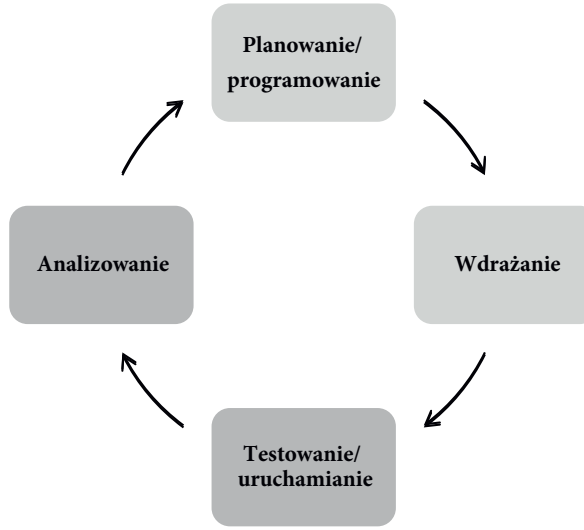
- analiza (zagrożenia, posiadane siły i środki, dotychczasowe efekty stosowania planu itp.);
- sporządzenie planu (lub korekta);
- wdrożenie planu (przeszkolenie ludzi, zmiany techniczne i organizacyjne itp.);
- wykonanie (lub testowanie w ramach ćwiczeń);
- ponowna analiza itd.

Wprowadzone do definicji „programowanie" wskazuje, że w ramach zarządzania kryzysowego realizuje się dwa cykle planistyczne. Pierwszy odnosi się do działań operacyjnych i dotyczy krótszej perspektywy czasowej. Programowanie, którego przykładem może być Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), odnosi się do opracowywania dokumentu strategicznego o większym poziomie ogólności i dłuższej perspektywie czasowej na jego realizację. Mimo to taki dokument również powinien być opracowywany z zachowaniem cyklu działania zorganizowanego.

Plan, który nie został oparty na cyklu działania zorganizowanego, często wywołuje tzw. syndrom papierowego planu (Auf der Heide 1989) – decydent, który interesował się możliwymi zagrożeniami i ich skutkami, wiedząc, że powstał plan, uznaje błędnie, iż problem przestał istnieć. W rzeczywistości sam dokument planistyczny jest jedynie podręcznikiem szkoleniowym i ewentualnie podstawą do zmian techniczno-organizacyjnych. Zaś prawidłowo przeszkolony zespół sięga do planu jedynie w wyjątkowych przypadkach, gdyż zadania w nim zawarte ma opanowane w drodze ćwiczeń. Właśnie odpowiednie przygotowanie zespołów ludzkich jest właściwym celem planowania. Jednym z pierwszych, którzy to zauważyli, był generał Dwight D. Eisenhower. Według jego słów: „Plany są niczym, planowanie jest wszystkim" (Eisenhower 1958).

Konieczność wdrożenia zintegrowanego (czyli wielopodmiotowego i wielopoziomowego) planowania można zamknąć w stwierdzeniu, że wszystkie działania wspólne powinny być wspólnie przygotowane, wdrożone, przetestowane i zrealizowane. Można zatem przyjąć, że plan jest środkiem, cykl planowania metodą, zaś ostatecznym celem planowania jest wyszkolenie i wyposażenie zespołów ludzkich przewidywanych do reagowania w sytuacjach kryzysowych. Cykl planowania zobrazowano na schemacie nr 3.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353



Schemat 3. Cykl planowania

Źródło: opracowanie własne

1.7.2. Raport o zagrożeniach bezpieczeństwa narodowego

Planowanie działań na poszczególnych szczeblach administracji publicznej nie może być realizowane w sposób autonomiczny. Plany powinny być ze sobą spójne co do wskazania celów działania. W razie braku tej spójności mogłaby powstać sytuacja, w której przykładowo gminny plan przeciwpowodziowy zakłada obronę polderów przed zalaniem, a plan wojewódzki uznaje, że poldery należy celowo zalać w celu ochrony obszarów ważniejszych z gospodarczego bądź społecznego punktu widzenia. Ponadto powielanie tych samych pozycji magazynowych czy sprzętu ratowniczego na szczeblu gminy, powiatu i województwa jest ekonomicznie nieuzasadnione. Pamiętając o definicji sytuacji kryzysowej, a zwłaszcza o zapisanej w niej nieadekwatności posiadanych sił i środków (co stanowi o istocie sytuacji kryzysowej), można przyjąć, że siły i środki ujęte w planie na wyższym poziomie powinny stanowić uzupełnienie zasobów przygotowanych przez szczebel niższy. Z drugiej strony cele działania ujęte w planie niższego szczebla nie mogą być sprzeczne z celami przyjętymi na szczeblu wyższym. Nie zawsze bowiem niekorzystny rozwój sytuacji ma przebieg „z dołu do góry". Często informacje o możliwości wystąpienia sytuacji kryzysowej otrzymują najpierw wyższe szczeble administracji i to one będą uruchamiać niezbędne przedsięwzięcia.

Aby osiągnąć spójność poszczególnych planów przyjęto w ustawie, że są one oparte na wspólnych dokumentach wyjściowych. Dokumentami tymi są:

- wnioski z raportu o zagrożeniach bezpieczeństwa narodowego (UZK, art. 5a);
- wytyczne ministra właściwego do spraw administracji publicznej (dla planów wojewódzkich) (UZK, art. 13 ust. 3);

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

– zalecenia wojewody (dla planów powiatowych) (UZK, art. 14 ust 2 pkt 2 lit. a);
– zalecenia starosty (dla planów gminnych) (UZK, art. 17 ust 2 pkt 2 lit. c).

W efekcie powstał mechanizm zapewniający spójność planów sporządzanych na bazie ustaw branżowych oraz ujednolicenie celów działania i zasobów niezbędnych do ich osiągnięcia.

Jednak warunkiem, bez którego trudno mówić o właściwym przygotowaniu na ewentualne zagrożenia, jest wiedza o ich rodzaju i prawdopodobieństwie wystąpienia. Wiedza ta jest rozproszona pomiędzy różnymi służbami, inspekcjami i strażami oraz administracją działającą na wszystkich szczeblach. Dlatego dokumentem inicjującym proces planowania w ramach systemu zarządzania kryzysowego jest Raport o zagrożeniach bezpieczeństwa narodowego (UZK, art. 5a ust. 1). Raport, a raczej jego części składowe (raporty cząstkowe), są sporządzane zarówno przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych, jak i wojewodów. Jest on jedynym takim przekrojowym dokumentem opracowywanym na poziomie krajowym. Pokazuje, jaka jest percepcja zagrożeń oraz ocena ich negatywnych skutków na poziomie centralnym i wojewódzkim. Daje to też możliwość porównania, czy postrzeganie zagrożeń na szczeblu wojewódzkim koreluje z zagrożeniami ujętymi w raportach cząstkowych organów centralnych. W efekcie jest jedynym takim przekrojowym dokumentem opracowywanym na poziomie krajowym obrazującym całościowo zagrożenia i ryzyko z nimi związane. Jego rangę podkreśla też fakt, że jest dokumentem rządowym, przyjmowanym przez Radę Ministrów w drodze uchwały[8].

Ponadto zgodnie z rozporządzeniem raporty cząstkowe mają być wykonywane zgodnie z właściwością rzeczową poszczególnych organów (DzU z 2010 r. nr 83, poz. 540, § 3 ust. 1). Oznacza to, że zgodnie z zamysłem ustawodawcy w trakcie powstawania raportu nastąpi proces analizowania zagrożeń na kolejnych szczeblach administracji, którego efekty mogą zostać wykorzystane nie tylko przy tworzeniu całościowego raportu, lecz także poszczególnych planów zarządzania kryzysowego.

Ze względu na fakt, że dokument opracowuje kilka podmiotów, RCB zostało wskazane jako instytucja koordynująca jego przygotowanie (Skomra 2017 d). W ustawie przewidziano natomiast, że w części dotyczącej zagrożeń terrorystycznych za koordynację odpowiada Szef Agencji Bezpieczeństwa Wewnętrznego.

Należy też zauważyć, że pomysł na wskazanie instytucji koordynującej na potrzeby opracowania takiego rodzaju dokumentu nie jest rozwiązaniem unikalnym na tle innych krajów europejskich. Wpisuje się również w rozwiązania zaproponowane przez Komisję Europejską. W dokumencie pt. *Risk Assessment and Mapping Guidelines for Disaster Management* zapisano, że „pierwszym krokiem w ramach procesu

[8] Do tej pory Rada Ministrów przyjęła trzy uchwały w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego – 24 czerwca 2011 r., 12 lipca 2013 r. oraz 15 września 2015 r.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

opracowania krajowej oceny ryzyka powinno być wyznaczenie jednej instytucji, która będzie koordynować pracę pozostałych podmiotów" (*Risk Assessment…*, s. 12).

Ciekawym rozwiązanym przyjętym w UZK jest wyszczególnienie odrębnego koordynatora w postaci Szefa Agencji Bezpieczeństwa Wewnętrznego. Intencją ustawodawcy było wskazanie specyficznego charakteru zagrożeń terrorystycznych w ramach zarządzania kryzysowego, jako wymagającego szczególnej, odmiennej koordynacji działań o odmiennym, specjalnym i najczęściej niejawnym charakterze, często wymagającym kooperacji międzynarodowej. Wyznaczenie szefa ABW jako podmiotu właściwego do koordynacji tego typu działań jest logiczną konsekwencją posiadanych przez ABW uprawnień i prowadzonych działań. Nie oznacza to jednak, że część raportu dotycząca zagrożeń terrorystycznych będzie odrębnym, autorskim dokumentem ABW. Przeciwnie, zgodnie z brzmieniem cytowanego artykułu to dyrektor RCB ma decydujący wpływ na całościowy charakter i kształt raportu również w części koordynowanej przez szefa ABW. Aby uniknąć wątpliwości w tym zakresie, rozporządzenie wykonawcze ustala, że każdy z wykonawców przygotowuje tylko jeden raport cząstkowy, który trafia do dyrektora RCB. Jedynie wówczas, gdy w raporcie wskazano na zagrożenia o charakterze terrorystycznym mogące doprowadzić do sytuacji kryzysowej, raport otrzymuje również szef ABW (DzU z 2010 r. nr 83, poz. 540, § 7 ust. 1).

Tworzenie Raportu o zagrożeniach bezpieczeństwa narodowego jest procesem złożonym, wieloetapowym i systematycznym. Najistotniejsza część pracy nad dokumentem odbywa się podczas opracowywania raportów cząstkowych. W każdej z instytucji prowadzone są wówczas prace merytoryczne mające na celu wskazanie możliwych zagrożeń oraz pozostałych elementów Raportu w zakresie jej działalności. Na tym etapie tworzenia dokumentu powinno zostać zaangażowane jak najszersze grono specjalistów. W szczególności powinni być to pracownicy danej instytucji. Co więcej, wtedy też pracownicy administracji publicznej powinni współpracować z sektorem prywatnym (np. operatorami infrastruktury krytycznej działającymi na terenie województwa lub w stosunku do których minister jest właścicielem), środowiskiem naukowym (np. z pracownikami podległych lub nadzorowanych instytutów naukowo-badawczych lub z przedstawicielami szkół wyższych funkcjonujących na terenie danego województwa) oraz z organizacjami pozarządowymi. Optymalnym rozwiązaniem jest tworzenie tematycznych grup roboczych w zakresie poszczególnych zagrożeń.

Kluczową rolę w opracowywaniu raportów cząstkowych ma więc szczebel ekspercki. Jednakże w ustawie zostały przewidziane też zadania w tym zakresie dla średniego i wyższego poziomu decyzyjnego. Mianowicie funkcjonujące w ministerstwach i urzędach centralnych zespoły zarządzania kryzysowego są zobowiązane do „dokonywania okresowej oceny zagrożeń na potrzeby Raportu" (UZK, art. 12c ust. 1). W praktyce oznacza to, że przed zatwierdzeniem raportu cząstkowego przez ministra lub kierownika urzędu centralnego powinien on zostać zaopiniowany (uzupełniony/skorygowany) przez zespół.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Na podstawie skorygowanych raportów w Rządowym Centrum Bezpieczeństwa jest opracowywany projekt Raportu o zagrożeniach bezpieczeństwa narodowego. Następnie dokument przechodzi standardowy proces legislacyjny (uzgodnienia międzyresortowe, uzgodnienia przed Komitetem Stałym Rady Ministrów). Podczas niego wykonawcy raportów cząstkowych mogą wnosić uwagi i uzupełnienia do całościowego dokumentu. Następnie uzgodniony dokument jest przekazywany do przyjęcia, w formie uchwały, przez Radę Ministrów.

Przewidziany przez UZK proces tworzenia Raportu o zagrożeniach bezpieczeństwa narodowego jest procesem cyklicznym. Oznacza to, że możliwe zagrożenia muszą być systematycznie monitorowane i analizowane zarówno przez pracowników administracji centralnej, jak i wojewódzkiej. Dlatego przewidziany został dwuletni cykl aktualizacyjny (UZK, art. 5a).

Wymienione w art. 5a UZK elementy składowe Raportu o zagrożeniach bezpieczeństwa narodowego zostały doprecyzowane w § 4 rozporządzenia RM w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego. Wskazano, że w raportach cząstkowych powinny być ujęte następujące rodzaje zagrożeń:

- takie, które mogą w istotny sposób wpłynąć na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogą mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego;
- takie, których skutki mogą:
  - godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, a w szczególności w suwerenność, niepodległość i nienaruszalność terytorium;
  - zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach;
  - oddziaływać, obok Rzeczypospolitej Polskiej, także na inne państwa;
  - dotyczyć terytorium Rzeczypospolitej Polskiej lub jej obywateli, mimo możliwego wystąpienia w innym państwie;
- występujące w rejonach napięć, konfliktów i kryzysów międzynarodowych, mające wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych;
- o charakterze terrorystycznym mogące doprowadzić do sytuacji kryzysowej.

Warto zwrócić uwagę, że większość wskazanych powyżej zagrożeń wykracza poza potocznie rozumiane zadania dla zarządzania kryzysowego, a utożsamianie z klęskami żywiołowymi i awariami technicznymi. Te zadania właściwie odnoszą się tylko do pkt 1 lit. b, czyli do zagrożeń, których skutki mogą zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach[9].

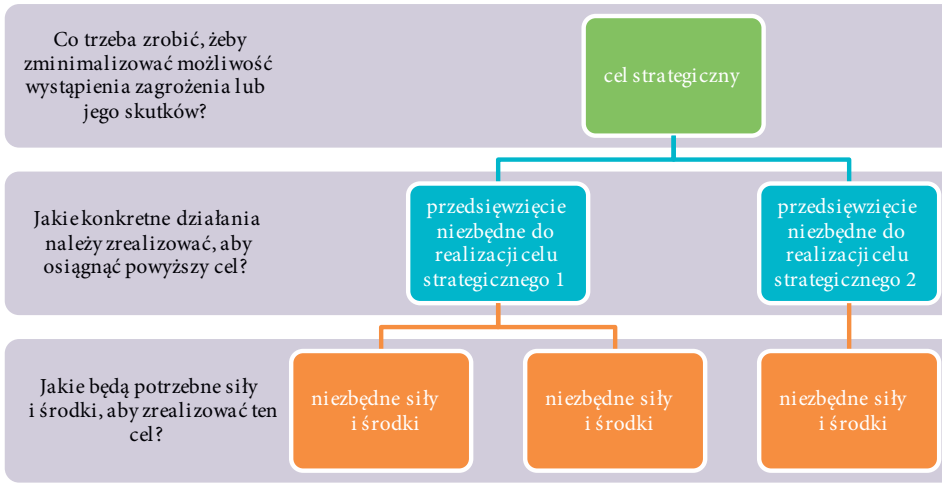
[9] Wymieniona w pkt 1 lit. b, kategoria zagrożeń jest zbieżna z definicją klęski lub katastrofy zawartą w UMOL, przez którą rozumie się dowolną sytuację, która ma lub może mieć poważne skutki dla ludzi, środowiska naturalnego lub mienia, w tym dziedzictwa kulturowego.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zdecydowana większość zagrożeń wiąże się z szeroko rozumianym bezpieczeństwem państwa. Odnoszą się więc one do takich wartości jak suwerenność, niepodległość, nienaruszalność terytorium czy też do kwestii związanych z potencjałem ekonomicznym i obronnym oraz z międzynarodową pozycją kraju. W rozporządzeniu uwzględniono też zagrożenia transgraniczne, które z jednej strony mogą dotyczyć terytorium RP lub jej obywateli, mimo możliwego wystąpienia w innym państwie, z drugiej zaś oddziaływać, obok RP, także na inne państwa. Na uwagę zasługuje w szczególności punkt dotyczący zagrożeń nie tyle dla państwa, ile dla obywateli RP mogących znajdować się poza granicami kraju.

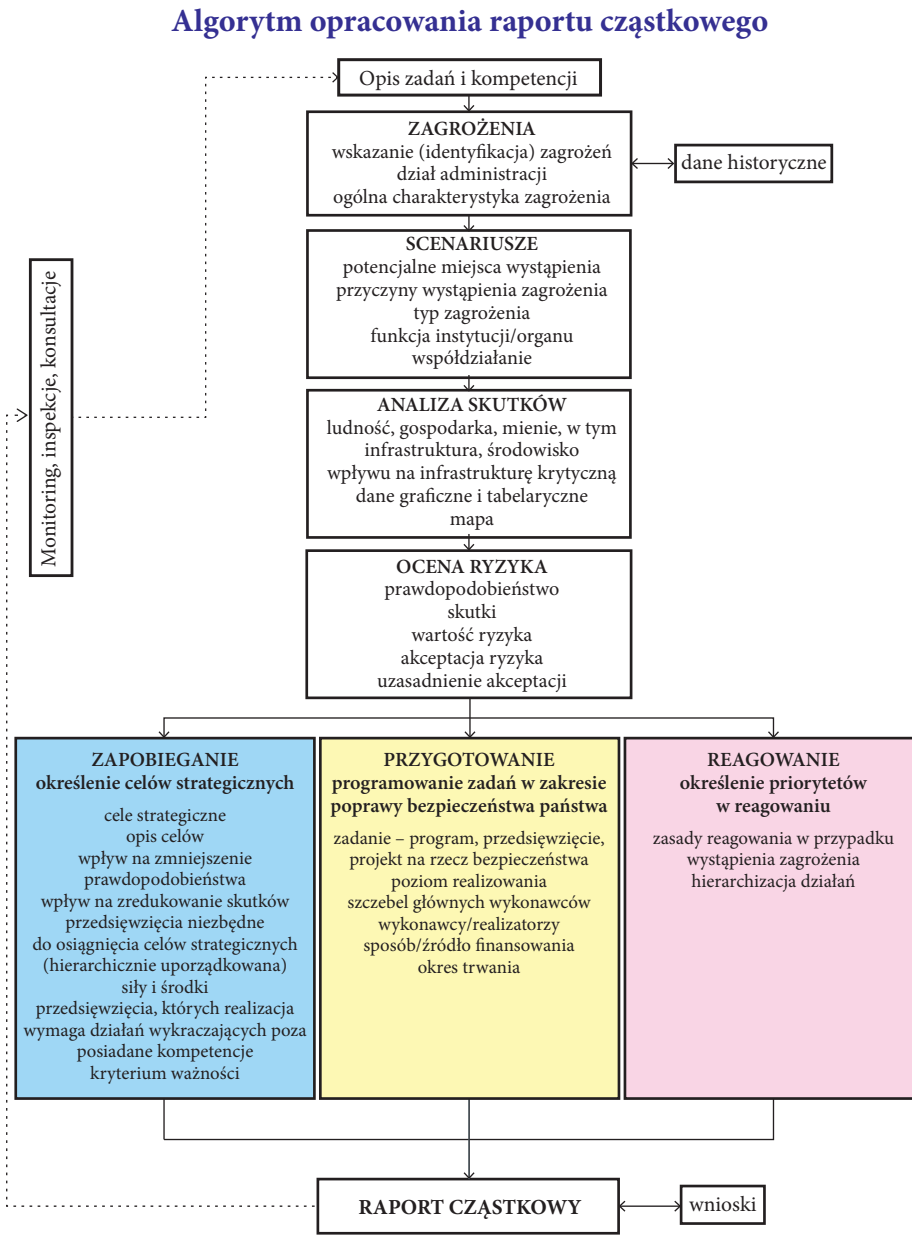
W UZK przyjęto, że w Raporcie poza wskazaniem możliwych zagrożeń zostaną też określone działania, które miałyby im przeciwdziałać. Zadaniem Raportu jest więc zdefiniowanie tzw. celów strategicznych, czyli określenie, jakie działania należy podjąć, aby zminimalizować możliwość wystąpienia zagrożenia lub ograniczyć jego skutki. Cele te powinny być uporządkowane według ich ważności. Dla każdego zagrożenia należy wskazać cel priorytetowy z punktu widzenia bezpieczeństwa narodowego. Dla wszystkich celów strategicznych wskazuje się siły i środki niezbędne do ich osiągnięcia oraz uporządkowane przedsięwzięcia, które muszą zostać zrealizowane, aby cele mogły zostać osiągnięte.

W tym miejscu wykonawcy raportów cząstkowych powinni zwrócić uwagę na przedsięwzięcia wykraczające poza ich kompetencje i wymagające podjęcia działań przez inne podmioty (możliwa jest sytuacja, w której dane zagrożenie zostało zidentyfikowane przez podmiot opracowujący raport, jednak działania, jakie mogłyby zmniejszyć prawdopodobieństwo jego wystąpienia lub zmniejszyć możliwe negatywne skutki, nie leżą w jego możliwościach działania). Etapy opracowywania raportu cząstkowego po zidentyfikowaniu zagrożenia przedstawiono na schemacie nr 4.


Co trzeba zrobić, żeby zminimalizować możliwość wystąpienia zagrożenia lub jego skutków?
cel strategiczny
Jakie konkretne działania należy zrealizować, aby osiągnąć powyższy cel?
przedsięwzięcie niezbędne do realizacji celu strategicznego 1
przedsięwzięcie niezbędne do realizacji celu strategicznego 2
Jakie będą potrzebne siły i środki, aby zrealizować ten cel?
niezbędne siły i środki
niezbędne siły i środki
niezbędne siły i środki

Schemat 4. Działania wynikające ze zidentyfikowania zagrożenia
Źródło: opracowanie własne

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353



Schemat 5. Algorytm opracowania raportu cząstkowego
Źródło: „Procedura…”

W RoZBN dla każdego rodzaju zagrożeń wskazuje się ponadto programy realizowane na poziomie krajowym, wojewódzkim, powiatowym i gminnym, których celem jest poprawa bezpieczeństwa. Wyszczególniane są również instytucje realizujące poszczególne programy (na poziomie rządowym, samorządowym oraz

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

pozarządowe) oraz okres trwania tych programów. Ten zabieg pozwala zidentyfikować ewentualne luki w działaniach związanych z zapobieganiem możliwym zagrożeniom i przygotowaniem się na nie (w przypadku gdy dane zagrożenie zostało zidentyfikowane i ocenione jako poważne przez wykonawców raportów cząstkowych, a obecnie nie są podejmowane żadne działania, które miałyby mu przeciwdziałać). Ta część pozwala więc odpowiedzieć na pytanie: co nam grozi i czy oraz co obecnie z tym robimy.

Ostatnia część raportu określa priorytety w reagowaniu na zagrożenia. Są to zarówno zasady reagowania w przypadku wystąpienia zagrożenia, jak i hierarchizacja działań. Powinny stanowić podstawę do procedur reagowania kryzysowego zawartych w planach zarządzania kryzysowego.

Warto zauważyć, że główną osią budowy RoZBN są zagrożenia. To z nich wynikają i im są podporządkowane wszystkie pozostałe części dokumentu. Według tej zasady w 2010 r. w RCB została opracowana „Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego". W procedurze zawierającej zarówno część opisową (instrukcję), jak i część w formie tabelarycznej (do wypełnienia) określono sposób przygotowania raportu. Kolejne kroki prowadzące do opracowania raportu cząstkowego ilustruje schemat 5.

Każdy z ministrów, kierowników urzędów centralnych oraz wojewodowie dokonują analizy i oceny możliwości wystąpienia powyższych kategorii zagrożeń w zakresie swojej odpowiedzialności. Zgodnie z „Procedurą…" dla każdego zidentyfikowanego zagrożenia wskazuje się jego możliwe scenariusze (od 2 do 3) wraz z ich szczegółowym opisem. W opisie powinny się znaleźć potencjalne miejsca wystąpienia danego zdarzenia oraz jego możliwe przyczyny. Analizowane są również możliwe skutki dla ludności, gospodarki, mienia i infrastruktury oraz środowiska. Dla każdej z tych kategorii powinny zostać wskazane zarówno skutki bezpośrednie (odczuwalne natychmiast), jak i pośrednie (odłożone w czasie).

W ramach analizy skutków dla ludzi wykonawcy raportów cząstkowych powinni uwzględnić w szczególności potencjalną liczbę:

- ofiar śmiertelnych,
- rannych lub poważnie chorych (wymagających hospitalizacji),
- ewakuowanych.

Ponadto w zakresie skutków pośrednich powinny zostać również wskazane skutki społeczne (np. możliwy wzrost bezrobocia), a także skutki związane z trwałą niezdolnością do pracy oraz skutki psychologiczne. W części mającej na celu analizę skutków dla gospodarki sporządzający raporty cząstkowe powinni przedstawić zarówno możliwe skutki krótkotrwałe, jak i długoterminowe.

Następnie, podczas analizy skutków dla mienia, w tym infrastruktury, powinny zostać określone potencjalne zakłócenia lub zniszczenia, jakie mogą wystąpić w wyniku zaistnienia zidentyfikowanego zagrożenia. Zgodnie z „Procedurą…" wykonawcy raportów cząstkowych powinni uwzględnić skutki bezpośrednie,

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

skutki pośrednie (efekt domina) lub skutki odłożone w czasie. O ile jest to możliwe, wskazuje się szacunkowe koszty strat oraz koszty odbudowy.

Podczas analizy skutków dla środowiska, oprócz określenia niekorzystnego wpływu danego scenariusza na środowisko, powinno zostać określone, które skutki są odwracalne/odnawialne, a które powodują całkowite zniszczenie/degradację środowiska. Przy opisie powinny zostać też wskazanie możliwe przedziały czasowe.

Ostatnim etapem analizy skutków jest opis, w jaki sposób zdarzenie może niekorzystnie wpłynąć na infrastrukturę krytyczną. Określa się, czy dany scenariusz wpływa na funkcjonowanie infrastruktury krytycznej oraz wskazuje potencjalnie narażone systemy IK. Zgodnie z UZK infrastrukturę krytyczną rozumie się jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Zagadnienia związane z wyłanianiem obiektów IK i zasadami ich ochrony zostaną omówione w jednym z kolejnych rozdziałów.

Zgodnie z „Procedurą…" wszystkie opisane powyżej analizy powinny zostać uzasadnione wszystkimi dostępnymi danymi (np. ekspertyzy w formie opisowej, graficznej lub tabelarycznej), na których podstawie został opracowany dany scenariusz. O ile jest taka możliwość, wykonawcy raportów cząstkowych powinni dołączyć mapy przedstawiające strefę/zasięg zagrożenia dla danego scenariusza.

Wykonawcy raportów cząstkowych powinni również wskazać, czy dany scenariusz został ujęty w resortowym lub wojewódzkim planie zarządzania kryzysowego oraz czy powinien znaleźć się w Krajowym Planie Zarządzania Kryzysowego. W ten sposób sporządzający raporty mają możliwość odpowiedzi na pytanie, czy posiadaliby wystarczające (adekwatne) kompetencje oraz siły i środki, aby przeciwdziałać danemu zagrożeniu (scenariuszowi) w wypadku jego wystąpienia; czy sytuacja wymagałaby współdziałania kilku ministrów, kierowników urzędów centralnych i/lub wojewodów oraz czy byłaby niezbędna koordynacja ich działań, a także czy istniałaby potrzeba użycia dodatkowych sił i środków.

Kolejnym krokiem przewidzianym w „Procedurze…" jest analiza ryzyka dla poszczególnych scenariuszy. Na potrzeby opracowania RoZBN przyjęto, że ryzyko jest rozumiane jako prawdopodobieństwo wystąpienia niekorzystnego zdarzenia wraz z jego skutkami w określonym czasie[10].

Dla określania prawdopodobieństwa przyjęto następującą skalę jakościową (opisową) („Procedura…", s. 14):

[10] Definicja ta jest zbieżna zarówno z definicją ujętą w opracowanych przez Komisję Europejską wskazówkach *Risk Assessment and Mapping Guidelines for Disaster Management*, jak i z pośrednio zdefiniowanym ryzykiem w UMOL.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 4. Ocena prawdopodobieństwa wystąpienia zdarzenia

Skala	*Prawdopodobieństwo*	*Opis*
1	Bardzo rzadkie	Może wystąpić tylko w wyjątkowych okolicznościach. Może wystąpić raz na pięćset lub więcej lat.
2	Rzadkie	Nie oczekuje się, że się może zdarzyć i/lub nie jest w ogóle udokumentowane, nie istnieje w przekazach ludzi, i/lub zdarzenia nie wystąpiły w podobnych organizacjach, urządzeniach, społecznościach, i/lub istnieje mała szansa, powód czy też inne okoliczności, aby zdarzenia mogły wystąpić. Mogą one wystąpić raz na sto lat.
3	Możliwe	Może zdarzyć się w określonym czasie i/lub przypadkowo, zdarzenia są rzadko udokumentowane lub cząstkowo przekazywane w formie ustnej, i/lub bardzo mało zdarzeń, i/lub jest pewna szansa, powód czy też urządzenia powodujące, że zdarzenie może wystąpić. Może zdarzyć się raz na dwadzieścia lat.
4	Prawdopodobne	Jest prawdopodobne, że wystąpi w większości okoliczności i/lub zdarzenia są systematycznie dokumentowane i przekazywane w formie ustnej, i/lub występuje znaczna szansa, powód lub urządzenia pozwalające na jego wystąpienie. Może zdarzyć się raz na pięć lat.
5	Bardzo prawdopodobne	Oczekuje się, że zdarzy się w większości okoliczności i/lub zdarzenia te są bardzo dobrze udokumentowane, i/lub funkcjonują wśród mieszkańców i są przekazywane w formie ustnej. Może wystąpić raz na rok lub częściej.

Źródło: „Procedura…"

Natomiast klasyfikację dla określenia skutków przedstawia tabela nr 2 („Procedura…", s. 16).

Tabela 5. Ocena skutków zdarzenia

Skala	*Skutki*	*Kat.*	*Opis* **(Z – życie i zdrowie, M – mienie, S – środowisko)**
A	Nieistotne	**Z**	Nie ma ofiar śmiertelnych i rannych. Nikt lub mała liczba ludzi została przemieszczona na krótki okres (do 2 godzin). Nikt nie wymaga lub niewielka liczba osób wymaga pomocy (nie finansowej lub materialnej).
		M	Praktycznie bez zniszczeń. Brak wpływu lub bardzo niewielki wpływ na społeczność lokalną. Brak lub niewielkie straty finansowe.
		S	Niemierzalny efekt w środowisku naturalnym.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

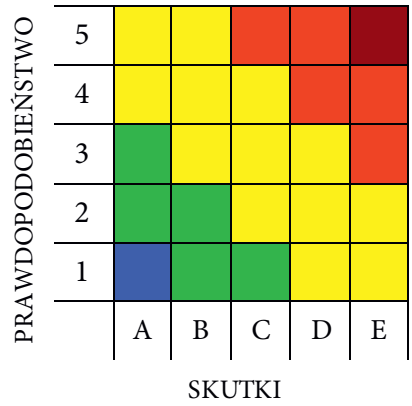
Skala	*Skutki*	*Kat.*	*Opis* **(Z – życie i zdrowie, M – mienie, S – środowisko)**
B	Małe	**Z**	Mała liczba rannych, lecz bez ofiar śmiertelnych. Wymagana pierwsza pomoc. Konieczne przemieszczenia ludzi (na krócej niż 24 godziny). Część ludzi potrzebuje pomocy.
		M	Występują pewne zniszczenia. Występują pewne utrudnienia (nie dłużej niż 24 godziny). Niewielkie straty finansowe. Niewymagane dodatkowe środki.
		S	Niewielki wpływ na środowisko naturalne o krótkotrwałym efekcie.
C	Średnie	**Z**	Potrzebna pomoc medyczna, lecz bez ofiar śmiertelnych. Niektórzy wymagają hospitalizacji. Potrzebne dodatkowe miejsca w szpitalach oraz dodatkowy personel medyczny. Przebywanie ewakuowanych ludzi w wyznaczonych miejscach z możliwością powrotu w ciągu 24 godzin.
		M	Ustalenie miejsc zniszczeń, które wymagają rutynowej naprawy. Normalne funkcjonowanie społeczności z niewielkimi niewygodami. Spore straty finansowe.
		S	Pewne skutki w środowisku naturalnym, lecz krótkotrwałe lub małe skutki o długotrwałym efekcie.
D	Duże	**Z**	Mocno poranieni, dużo osób hospitalizowanych, duża liczba osób przemieszczonych (na dłużej niż 24 godziny). Ofiary śmiertelne. Potrzeba szczególnych zasobów do pomocy ludziom i do usuwania zniszczeń.
		M	Społeczność częściowo niefunkcjonująca, niektóre służby są nieosiągalne. Duże straty finansowe. Potrzebna pomoc z zewnątrz.
		S	Długotrwałe efekty w środowisku naturalnym.
E	Katastrofalne	**Z**	Duża liczba poważnie rannych. Duża liczba hospitalizowanych. Ogólne i długotrwałe przemieszczenie ludności. Duża liczba ofiar śmiertelnych. Wymagana duża pomoc dla dużej liczby ludzi.
		M	Rozległe zniszczenia. Niemożność funkcjonowania społeczności bez istotnej zewnętrznej pomocy.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Skala	*Skutki*	*Kat.*	*Opis* **(Z – życie i zdrowie, M – mienie, S – środowisko)**
		S	Duży wpływ na środowisko naturalne i/lub stałe zniszczenia.

Źródło: „Procedura…"

W konsekwencji określenia poziomu prawdopodobieństwa i skutków możliwe jest wskazanie wartości ryzyka. Wartość ryzyka dla każdego scenariusza jest wskazywana na matrycy ryzyka pokazującej zależność między prawdopodobieństwem a skutkami.



Rys. 2. Matryca ryzyka

Źródło: „Procedura…"

Legenda:
niebieski – ryzyko minimalne
zielony – ryzyko małe
żółty – ryzyko średnie
czerwony – ryzyko duże
brunatny – ryzyko ekstremalne

Kolejnym etapem jest oszacowanie ryzyka i wskazanie poziomu jego akceptacji. W „Procedurze…" przyjęte zostały 4 kategorie akceptowalności ryzyka:

- ryzyko akceptowane (A) – nie są wymagane żadne dodatkowe środki bezpieczeństwa, akceptowane są aktualne rozwiązania oraz przypisane im siły i środki, działania monitorujące;
- ryzyko tolerowane (dopuszczalne) (T) – należy dokonać oceny alternatyw, czy wprowadzenie niewielkich zmian organizacyjnych, prawnych bądź funkcjonalnych nie przyczyni się do poprawy bezpieczeństwa lub jego poczucia;
- ryzyko warunkowo tolerowane (WT) – należy wprowadzić dodatkowe środki bezpieczeństwa w terminie 6 miesięcy, należy ulepszyć stosowane rozwiązania;

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

– ryzyko nieakceptowane (N) – należy podjąć natychmiastowe działania w celu zwiększenia bezpieczeństwa, wprowadzić dodatkowe/ nowe rozwiązania („Procedura…", s. 17–18).

Wykonawcy raportów cząstkowych zostali też zobowiązani do uzasadnienia, dlaczego wskazali taki, a nie inny poziom akceptacji ryzyka. W przypadku poziomu akceptowanego oraz tolerowanego uzasadnienia mają charakter pozytywny (np. funkcjonują odpowiednie rozwiązania prawne, właściwe instytucje dysponują wystarczającymi kompetencjami, siłami i środkami, funkcjonuje system monitorowania zagrożeń, ostrzegania i alarmowania itp.), natomiast w przypadku ryzyka warunkowo tolerowanego oraz nieakceptowalnego – charakter negatywny (np. brakuje odpowiedniej infrastruktury oraz środków technicznych, takich jak wały przeciwpowodziowe, zbiorniki retencyjne lub są one przestarzałe, ludzie zamieszkujący na danym terenie nie mają świadomości zagrożeń i/lub nie wiedzą, jak postępować w przypadku ich wystąpienia).

Akceptacja poziomu ryzyka jest zdecydowanie najtrudniejszym etapem całego procesu oceny ryzyka i prawie zawsze wymaga decyzji politycznej. Jest jednak jednym z wyzwań wynikających z obowiązywania UMOL. Zgodnie w nią państwa członkowskie mają obowiązek zarządzania ryzykiem. Jest on rozumiany jako „umiejętność państwa członkowskiego lub jego regionów do zmniejszenia ryzyka, dostosowania się do ryzyka lub ograniczenia ryzyka, w szczególności jego skutków i prawdopodobieństwa klęski lub katastrofy zidentyfikowanego w przeprowadzonej przez to państwo lub regiony ocenie ryzyka do poziomu akceptowanego w tym państwie członkowskim" (UMOL, art. 4 ust. 8). Państwa członkowskie zostały więc prawnie zobowiązane do przeprowadzenie ocen ryzyka rozumianych jako „całościowy, przekrojowy proces identyfikacji ryzyka, analizy ryzyka i szacowanie ryzyka podejmowany na szczeblu krajowym lub odpowiednim niższym szczeblu" (UMOL, art. 4 ust. 7). Oznacza to, że muszą wskazać najistotniejsze z punktu widzenia kraju „sytuacje, które mają lub mogą mieć poważne skutki dla ludzi, środowiska naturalnego lub mienia, w tym dziedzictwa kulturowego", dokonać analizy ich skutków oraz prawdopodobieństwa oraz określić, czy akceptują takie ryzyko.

Ponadto, zgodnie z Decyzją, oprócz oceny ryzyka państwa członkowskie zostały zobowiązane do sporządzenia planów zarządzania ryzykiem. Plany zarządzania powinny mieć na celu zarówno zapobieganie ryzyku (tj. powinny określać działanie mające na celu ograniczanie ryzyka lub łagodzenie negatywnych skutków klęsk żywiołowych i katastrof dla ludzi, środowiska naturalnego oraz mienia, w tym dziedzictwa kulturowego), jak i przygotowanie się na wypadek zaistnienia klęski lub katastrofy (tj. powinny określać odpowiedni stan zasobów ludzkich, środków materialnych, struktur, społeczności i organizacji).

Państwa członkowskie powinny być również w stanie, na podstawie zarówno dokonanej wcześniej oceny ryzyka, jak i planów zarządzania ryzykiem, realizować działania mające na celu zapobieganie ryzyku oraz przygotowanie się do skutecznego i szybkiego reagowania w przypadku klęsk lub katastrof.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

W tym miejscu należy zadać pytanie, czy Raport o zagrożeniach bezpieczeństwa narodowego wypełnia obowiązki nałożone przez decyzję w sprawie UMOL. Należy stwierdzić, że zdecydowanie nie, jednakże dokument ten można traktować jako punkt wyjścia do wypełnienia opisanych powyżej obowiązków.

Tabela 6. Porównanie obszaru objętego UZK i zakresem UMOL

Zagadnienie	*Mechanizm ochrony*	*Ustawa o zarządzaniu kryzysowym/rozporządzenie*	*Uwagi*
Co należy uwzględniać w krajowej ocenie ryzyka	klęski lub katastrofy – dowolna sytuacja, która ma lub może mieć poważne skutki dla ludzi, środowiska naturalnego lub mienia, w tym dziedzictwa kulturowego	zagrożenia, które mogą w istotny sposób wpłynąć na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogą mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego; zagrożenia, których skutki mogą: – godzić w bezpieczeństwo państwa, jego porządek konstytucyjny, a w szczególności w suwerenność, niepodległość i nienaruszalność terytorium, – zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach, – oddziaływać, obok RP, także na inne państwa, – dotyczyć terytorium RP lub jej obywateli, mimo możliwego wystąpienia w innym państwie; zagrożenia występujące w rejonach napięć, konfliktów i kryzysów międzynarodowych, mające wpływ na bezpieczeństwo państwa lub których potrzeba monitorowania i eliminacji wynika z podpisanych umów i traktatów międzynarodowych; zagrożenia o charakterze terrorystycznym mogące doprowadzić do sytuacji kryzysowej.	
Ocena ryzyka	całościowy, przekrojowy proces identyfikacji ryzyka, analizy ryzyka i szacowanie ryzyka podejmowany na szczeblu krajowym lub odpowiednim niższym szczeblu	termin pojawia się w UZK, brak jednak jego definicji; ujęta w UZK definicja map ryzyka: mapa lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę.	definicja oceny ryzyka z UMOL jest zbieżna z podejściem przyjętym w Procedurze opracowania raportu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zagadnienie	*Mechanizm ochrony*	*Ustawa o zarządzaniu kryzysowym/rozporządzenie*	*Uwagi*
Cykl oceny ryzyka	3 lata	2 lata	
Plany zarządzania ryzykiem	plany mające na celu zapobieganie ryzyku oraz przygotowanie się na nie	cele strategiczne w ramach RoZBN; plany zarządzania kryzysowego	
Podejmowanie środków	praktyczne wdrażanie tego, co zostało określone w ocenie ryzyka oraz wskazane w ramach planowania zarządzania ryzykiem		

Źródło: opracowanie własne

Jak wynika z tabeli nr 6 za spełniony można uznać jedynie jeden z trzech elementów zarządzania ryzykiem, tj. opracowywanie ocen ryzyka. Należy jednak zwrócić uwagę na znacznie szerszy zakres przedmiotowy RoZBN. W konsekwencji powstaje dokument o znacznie większym ciężarze gatunkowym, niż wymaga tego decyzja w sprawie UMOL. W znacznej większości RoZBN dotyka zagadnień o charakterze militarnym lub związanych z terroryzmem, co powoduje, że całość dokumentu ma charakter niejawny. W praktyce, zgodnie z art. 5a ust. 5 UZK, część zawierająca charakterystykę zagrożeń, których skutki mogą zagrozić życiu lub zdrowiu dużej liczby osób, mieniu w znacznych rozmiarach albo środowisku na znacznych obszarach, umieszczona zostaje w KPZK.

Ponadto należy też zwrócić uwagę, że pomimo braku ustawowej definicji oceny ryzyka, w „Procedurze…" przyjęto podejście zgodne zarówno z wskazówkami Komisji Europejskiej (*Risk Assessment and Mapping Guidelines for Disaster Management*), jak i z decyzją w sprawie UMOL, tj. procesu składającego się z trzech etapów – identyfikacji, analizy i szacowania ryzyka. Można więc przyjąć, że proces opracowania RoZBN w dużej mierze wypełnia obowiązek opracowania ocen ryzyka.

W kwestii planowania zarządzania ryzykiem można uznać, że w przypadku planów mających na celu zapobieganie ryzyku obowiązek ten jest fragmentarycznie realizowany przez określane w RoZBN cele strategiczne. Natomiast opracowywane na różnych szczeblach administracji plany zarządzania kryzysowego mogłyby częściowo wypełniać obowiązek w zakresie planów mających na celu osiągnięcie gotowości na wypadek klęsk lub katastrof.

Nie można w tym przypadku mówić jednak o zachowaniu pełnej spójności oraz wzajemnym uzupełnianiu się wszystkich wskazanych wyżej dokumentów. Nie ma też mechanizmu, dzięki któremu można byłoby sprawdzić (systematycznie monitorować), czy ujęte w RoZBN cele strategiczne są wdrażane oraz przede wszystkim – czy ich wdrożenie przyczyniło się do zmniejszenia ryzyka, dostosowania się do ryzyka lub jego ograniczenia.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Jeżeli chodzi o realizowanie działań mających na celu zapobieganie ryzyku oraz zapewnianie gotowości na podstawie opracowanej wcześniej oceny ryzyka oraz planów zarządzania ryzykiem, to należy stwierdzić, że na poziomie krajowym nie funkcjonuje obecnie taki systemowy mechanizm dla wszystkich rodzajów zagrożeń. Podejście, w którym realizowane inwestycje, w tym infrastrukturalne, są zaplanowaną konsekwencją przeprowadzonej wcześniej oceny ryzyka, a ich przeprowadzenie jest następnie monitorowane pod kątem przyczynienia się do zminimalizowania lub ograniczenia ryzyka, jest jednak niekiedy stosowane. Nie ma to charakteru systemowego, a zatem dotyczy albo wybranych jednostek organizacyjnych, albo wybranych rodzajów ryzyka (np. ryzyka powodziowego). Najczęściej stosowanie takiego podejścia wynika z wymogów UE.

Najważniejszym, a przy tym wymagającym największego doświadczenia i umiejętności analitycznych elementem raportu są wnioski odwołujące się do wcześniej wymienionych celów strategicznych. Tym razem w formie zhierarchizowanych przedsięwzięć niezbędnych do ich realizacji. W tym miejscu przede wszystkim należy uwzględnić wykaz zagrożeń, których uniknięcie, minimalizacja zasięgu lub skutków wymaga działań wykraczających poza posiadane kompetencje właściwych organów administracji publicznej. Należy też podać inne informacje, które zdaniem wykonawcy raportu całościowego lub cząstkowego mogą być przydatne przy tworzeniu KPZK (lub jego elementów), a także właściwych terytorialnie lub resortowo planów zarządzania kryzysowego.

W przyszłości należy rozważyć poszerzenie grupy podmiotów zaangażowanych w opracowanie raportu (opracowanie krajowej oceny ryzyka). Zgodnie z wskazówkami KE, rekomendacjami OECD oraz Ramowym programem z Sendai w opracowanie krajowej oceny ryzyka powinny być zaangażowane nie tylko podmioty administracyjne, lecz także przedstawiciele nauki, podmioty prywatne (na szczeblu krajowym powinni być to operatorzy infrastruktury krytycznej, na szczeblu samorządowym przedstawiciele podmiotów prywatnych istotnych z punktu widzenia funkcjonowania społeczności lokalnej), a także organizacje pozarządowe (w szczególności te, które uczestniczą w działaniach ratowniczych w przypadku wystąpienia klęsk lub katastrof, ale też np. takie, które prowadzą w tym zakresie działalność edukacyjną).

Na zakończenie informacji o raporcie należy zauważyć, że w celu dostosowania do wymogów UMOL konieczna będzie ustawowa zmiana zakresu lub charakteru raportu. Ani UZK, ani Raport nie zawierają definicji oceny ryzyka[11]. W UMOL ocena ryzyka oznacza całościowy, przekrojowy proces identyfikacji ryzyka, analizy ryzyka i szacowanie ryzyka podejmowany na szczeblu krajowym lub odpowiednim niższym

[11] Przygotowując się do realizacji zadań wynikających z UMOL, RCB zgłosiło do NCBiR projekt badawczy „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP". W chwili powstawania niniejszej książki prace nad projektem nadal trwały, niemniej jednak powstało już wiele przydatnych opracowań. Zob. szerzej: *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*, red. W. Skomra, SGSP 2015, *Pamięć przyszłości. Analiza ryzyka dla zarządzania kryzysowego*, red. G. Abgarowicz, Józefów 2015 oraz *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*, red. A. Kosieradzka, J. Zawiła-Niedźwiecki, edu-Libri, Kraków–Legionowo 2016.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

szczeblu. Ponadto celem sporządzenia oceny nie jest jedynie wiedza o potencjalnych zagrożeniach i ich skutkach. W myśl UMOL kraj członkowski UE powinien świadomie wpływać na poziom ryzyka, tworząc i realizując plany zarządzania ryzykiem.

W efekcie należy przewidywać, że dotychczasowy raport zostanie poszerzony o brakujące elementy i będzie podstawą do opracowania zarówno planów zarządzania kryzysowego, jak i planów zarządzania ryzykiem. W innym wariancie zamiast raportu powinien powstać nowy rządowy dokument strategiczny zawierający plany zarządzania ryzykiem na szczeblu krajowym.

1.7.3. Siatka bezpieczeństwa

Skoro plan zarządzania kryzysowego w założeniu integruje różne służby i podmioty (ich siły, środki i kompetencje), to podstawą takiego planu musi być dokument wskazujący, który organ czy służba w zależności od zagrożenia pełni rolę wiodącą, a który pomocniczą. W tym celu każdy plan musi zawierać siatkę bezpieczeństwa, przez którą w myśl ustawy należy rozumieć zestawienie zagrożeń ze wskazaniem podmiotu wiodącego przy ich usuwaniu oraz podmiotów współpracujących (UZK, art. 3).

W literaturze przedmiotu można znaleźć cały szereg różnych typów siatek bezpieczeństwa. Ich różnorodność wynika ze specyfiki działań, które opisują, oraz zależy od stopnia skomplikowania struktury organizacyjnej biorącej udział w działaniach. Przykłady siatek bezpieczeństwa przedstawiono w tabelach 6 do 11. Należy zwrócić uwagę na przykład zadaniowej (modułowej) siatki bezpieczeństwa przedstawionej w tabelach 9, 10 i 11. W myśl omawianego zapisu ustawowego siatka powinna być oparta na wyszczególnieniu zagrożeń. W siatkach zadaniowych odchodzi się od planowania opartego na zagrożeniach, a skupia na zadaniach i ich wykonawcach. I tak w pierwszym kroku (część pierwsza siatki modułowej) definiuje się wszystkie moduły niezbędne do prowadzenia działań wraz ze wskazaniem podmiotu wiodącego i wspomagających w każdym z nich. Niekiedy opis modułu jest wzbogacany szczegółową listą zadań do wykonania wraz z osobami odpowiedzialnymi za ich realizację. W drugim kroku (część druga siatki modułowej) do każdego zagrożenia wskazuje się moduły, jakie powinny zostać uruchomione i ewentualnie moduły przewidywane opcjonalnie. Takie podejście wymaga wprawdzie większej pracy planistycznej, ale jest bardziej praktyczne. Takie rozwiązanie zastosowano po raz pierwszy podczas Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012. Po opracowaniu planu zabezpieczenia turnieju przeprowadzono eksperyment w formie ćwiczeń Libero, w czasie których sprawdzono możliwości wykorzystania podejścia modułowego. Wykryte błędy skorygowano i poprawioną wersję planu poddano ponownemu testowaniu w formie ćwiczeń, a następnie wdrożono do użytku. Takie samo podejście zastosowano podczas planowania zabezpieczenia Światowych Dni Młodzieży w 2016 r. Obecnie podejście zadaniowe jest wdrażane w projekcie Krajowego Planu Zarządzania Kryzysowego oraz w planach zarządzania kryzysowego ministrów i kierowników urzędów centralnych. Wydaje się, że z czasem będzie to podstawowe podejście do budowania siatek bezpieczeństwa organów zarządzania kryzysowego.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 7. Przykład prostej siatki bezpieczeństwa dla fazy reagowania

Zdarzenie/podmiot	Organ administracji ogólnej *)	PSP – Krajowy System Ratowniczo-Gaśniczy	Jednostki ochrony ppoż. poza systemem	Policja	Pogotowie ratunkowe	Wojewódzki sztab wojskowy	Stacje ratownictwa chemicznego	Straż Graniczna	Inspektorat ochrony środowiska	Służby ratownicze PKP	Stacja sanitarno-epidemiologiczna	Lotnicze bazy leśne	Pogotowie gazowe	Pogotowie wodno-kanalizacyjne	Pogotowie energetyczne	Pogotowie ciepłownicze	Pogotowie dźwigowe	Inspektorat weterynarii	GOPR	WOPR	PCK	Inspektorat nadzoru budowlanego	Ratownictwo górnicze	Instytut Meteorologii i Gospodarki Wodnej	Właściciel, zarządca, organ założyciel-ski	Środki masowego przekazu
Pożar w rejonie zurbanizowanym	●	▲	○	○	○	●							●	●	●	●	●				●	●		●	●	
Pożar w przemyśle	●	▲	○	○	○	●	○	●	●					●	●						●				●	
Pożar wielkoobszarowy	●	▲	○	○	○	○		●	●	●		○						●			●				●	
Katastrofa chemiczno-ekologiczna	●	▲	○	○	○	●	○	●	●	●	●			●	●									○	●	●
Katastrofa w komuni-kacji drogowej	●	▲	●	○	○	●		●			●			●	●										●	●
Katastrofa w komuni-kacji kolejowej	●	○	●	○	○	●	●	●		▲	●				●						●				●	
Katastrofa budowlana	○	▲	●	○	○	●							●	●	●	●	●				●	○			●	
Zagrożenie radiacyjne	○	○	●	○	●	●	○	○	●	●	▲			●										○	●	●
Powódź	▲	○	○	○	○	○	○	●	●		●	○		●	●			●		●	●	●		○	●	

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zdarzenie/podmiot	Katastrofa na akwenie	Katastrofa lotnicza	Zaginięcie samolotów	Poszukiwanie osób zaginionych	Ratownictwo zwierząt	Atak terrorystyczny	Kryzys społeczny	Niekorzystne zjawisko atmosferyczne (gwałtowne opady, silne wiatry)	Masowa migracja do kraju
*Organ administracji ogólnej *)*	●	○		●	●	○	▲	○	○
PSP – Krajowy System Ratowniczo-Gaśniczy	▲	▲	○	○	▲	●	●	▲	
Jednostki ochrony ppoż. poza systemem		○	●	○	●	●	●	○	
Policja	○	○	○	▲	●	▲	●	●	○
Pogotowie ratunkowe	○	○	●			○	●	●	
Wojewódzki sztab wojskowy		○	▲	●			●		○
Stacje ratownictwa chemicznego						●			
Straż graniczna	●		●	●		●			▲
Inspektorat ochrony środowiska									
Służby ratownicze PKP						●			
Stacja sanitarno-epidemiologiczna									●
Lotnicze bazy leśne		●	○						
Pogotowie gazowe						●		○	
Pogotowie wodno-kanalizacyjne						●		○	
Pogotowie energetyczne						●			
Pogotowie ciepłownicze						●			
Pogotowie dźwigowe						●			
Inspektorat weterynarii					○	●			
GOPR		●	○	○					
WOPR	○		●	○					
PCK				●		●		●	○
Inspektorat nadzoru budowlanego								●	
Ratownictwo górnicze									
Instytut Meteorologii i Gospodarki Wodnej								○	
Właściciel, zarządca, organ zatoży-cielski		●			●			●	
Środki masowego przekazu			●	●			●	●	

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zagrożenie epidemiologiczne ludzi	○	●		●	●			●	▲									●		●									●
Zagrożenie epizootyczne zwierząt	●	●		●				●	●									▲											●
Unieszkodliwianie niebezpiecznych zwierząt		○	●	○	●													▲											●
Katastrofa geologiczna	▲	○		●	○			●	●			●	●																
Osoby chore psychicznie, usiłowania samobójcze		○		○	▲																								
Zagrożenie lodowe na rzekach	▲	●	●	●		○																							
Zagrożenie w przemyśle górniczym	●	○		●	●				○																				
Inne zagrożenia, w tym nieprzewidywalne	▲	○		○																									
Legenda	▲ Rola wiodąca								○ Rola pomocnicza																	● Współdziałanie według potrzeb				

Źródło: Skomra 2005, s. 177

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 8. Przykład siatki bezpieczeństwa dla obszaru województwa dla fazy reagowania

Lp.	*Uczestnik/ zagrożenie*	*Zagrożenie powodziowe*	*Zagrożenie radiacyjne*	*Wystąpienie chorób zakaźnych u ludzi*	*Zaistnienie poważnej awarii/poważnej awarii przemysłowej*	*Zagrożenie konstytucyjnego/zewnętrznego bezpieczeństwa*	*Zagrożenia klimatyczne*	*Katastrofa budowlana*	*Katastrofa komunikacyjna*	*Ograniczenia lub przerwy w dostawach paliw płynnych, energii elektrycznej, ciepła, gazu, wody*					*Rozległe awarie systemów łączności i teleinformatycznych*	*Choroby zakaźne u zwierząt*
										Sc 1	*Sc 2*	*Sc 3*	*Sc 4*	*Sc 5*		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	**Wojewoda**	W	W	W	PW	W	W	PW	PW	W	PW	PW	PW	PW	PW	PW
2	**PSP**	PW	PW		W		PW	W	W		PW				PW	PW
3	**PRM**	PW	PW	PW	PW		PW	PW	PW						PW	
4	**Policja**	PW	PW	PW	PW	PW		PW	PW	PW	PW				PW	PW
5	**Inspektorat ochrony środowiska**	PW			PW											
6	**Inspekcja Sanitarna**	PW	PW	PW												
7	**Inspekcja weterynaryjna**	PW														W
8	**IMGW**	PW					PW									
9	**RZGW**	PW														

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

10	**WZMiUW**	**PW**														
11	**SZ RP (WSzW)**	**PW**	**PW**	**PW**		**PW**	**PW**				**PW**			**PW**		
12	**ZOZ (publ. i niepubl.)**		**PW**	**PW**			**PW**	**PW**	**PW**							
13	**Prokuratura**					**PW**										
14	**ABW**					**PW**										
15	**Dostawcy z pkt. 11–15**									**PW**	**W**	**W**	**W**	**PW**		
16	**Operatorzy telekomuni-kacyjni**														**W**	
17	**WINB**							**PW**								
18	**PKP PLK SA**								**PW**							
19	**Port Lotniczy „Ławica”**								**PW**							
20	Ośrodek interwencji kryzysowej							PW	PW							
21	Inspekcja handlowa									PW						
22	Gmina	PW	PW	PW	PW	PW	PW	PW	PW	PW	PW	PW		W	PW	PW
23	Powiat	PW	PW	PW	PW	PW	PW	PW	PW	PW	PW	PW		PW	PW	PW

Legenda: W – podmiot wiodący; PW – podmiot współpracujący

Źródło: Plan zarządzania kryzysowego województwa wielkopolskiego z 2011 r.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 9. Przykład siatki bezpieczeństwa dla wszystkich czterech faz zarządzania kryzysowego (fragment)

Nr	Zdarzenie kryzysowe	Fazy zarządzania kryzysowego	MSW	MAiC	MZ	MŚ	MIiR	MRiRW	MON	MPiPS	MG	MF	MSP	MEN	MNiSW	MKiDN	MSZ	Rada Ministrów	RCB	Wojewoda
1	silne mrozy i opady śniegu	zapobieganie																	S	S
		przygotowanie																S	S	
		reagowanie																S	S	
		odbudowa																		
2	huragany	zapobieganie																		
		przygotowanie																S		
		reagowanie																		
		odbudowa																		
3	wielkoobszarowe pożary lasów	zapobieganie																		Starosta
		przygotowanie																		
		reagowanie																		
		odbudowa																		
4	epizootie	zapobieganie																		
		przygotowanie																		
		reagowanie															Insp. handl.			
		odbudowa																		

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Nr	Zdarzenie kryzysowe	Fazy zarządzania kryzysowego	MSW	MAiC	MZ	MŚ	MIiR	MRiRW	MON	MPiPS	MG	MF	MSP	MEN	MNiSW	MKiDN	MSZ	Rada Ministrów	RCB	Wojewoda
5	epifitozy	zapobieganie																		
		przygotowanie																	S	
		reagowanie																		
		odbudowa																		
6	katastrofy budowlane	zapobieganie																		
		przygotowanie																	S	
		reagowanie																		
		odbudowa																		
7	osuwiska	zapobieganie																		Staro-sta
		przygotowanie																	S	
		reagowanie																		
		odbudowa																	S	

Legenda: podmiot wiodący; podmiot współpracujący.

Źródło: KPZK 2013/2015

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 10. Przykład zadaniowej siatki bezpieczeństwa – cz. 1. Wykaz modułów wraz z ich wykonawcami

Lp.	*Moduł zadaniowy (mz)*	*Podmiot wiodący*	*Wykonawca*
1	Zarządzanie i koordynacja działań	Minister, wojewoda	Podmiot wiodący
2	Działania poszukiwawczo-ratownicze	MSW, wojewoda	Komendant Główny Państwowej Straży Pożarnej
3	Zabezpieczenie obiektów i terenów przed skutkami zalania w wyniku powodzi (katastrofalnego zatopienia)		
4	Ewakuacja ludności i zwierząt z zagrożonego rejonu		
5	Zwalczanie pożarów obiektów użyteczności publicznej i obiektów zamieszkania zbiorowego wykorzystywanych na potrzeby EURO 2012		
6	Zidentyfikowanie zagrożenia chemicznego, ograniczenie rozprzestrzeniania i zneutralizowanie/dekontaminacja skażenia		
7	Zapewnienie porządku publicznego w miejscu działania służb ratowniczych	MSW, wojewoda	Komendant Główny Policji
8	Przywrócenie zakłóconego porządku publicznego		
9	Ochrona mienia pozostawionego po ewakuacji ludności		
10	Uwolnienie zakładnika		
11	Zidentyfikowanie ofiar śmiertelnych		
12	Informowanie właściwych organów zagranicznych o ofiarach		
13	Neutralizacja zagrożenia bezprawnego użycia ładunku wybuchowego		
14	Zabezpieczenie przed dostępem osób postronnych rejonu skażenia chemicznego, skażenia i zakażenia biologicznego, skażenia promieniotwórczego		

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Lp.	Moduł zadaniowy (mz)	Podmiot wiodący	Wykonawca
15	Odblokowanie przejścia granicznego zablokowanego wskutek zakłócenia porządku publicznego/zwiększonego przemieszczania się dużych grup uczestników EURO 2012	MSW, wojewoda	Komendant Główny Straży Granicznej
16	Wzmocnienie kontroli granicznej w przypadku nagłego zagrożenia nielegalną migracją		
17	Umieszczenie dużej liczby cudzoziemców w strzeżonych ośrodkach dla cudzoziemców i aresztach w celu wydalenia		
18	Zapewnienie bezpieczeństwa zagrożonym osobom, obiektom i urządzeniom podlegającym ochronie	MSW	Szef Biura Ochrony Rządu
19	Zidentyfikowanie i ocena zagrożenia skażeniem promieniotwórczym	Prezes PAA	Prezes PAA
20	Ograniczenie skutków skażenia promieniotwórczego	MSW wojewoda	wojewoda
21	Dekontaminacja skażenia promieniotwórczego		KG PSP
22	Zapewnienie ratownictwa medycznego poszkodowanym	Minister Zdrowia, wojewoda	wojewoda
23	Analiza sytuacji epidemiologicznej oraz podjęcie działań zapobiegawczych i przeciwepidemicznych w przypadku wystąpienia groźnej choroby zakaźnej lub zakażenia u ludzi	Minister Zdrowia, wojewoda	Główny Inspektor Sanitarny, wojewoda
24	Dekontaminacja osób poszkodowanych w przypadku wystąpienia podejrzenia ich skażenia czynnikiem biologicznym		
25	Wycofanie z obrotu skażonych artykułów spożywczych		
26	Uruchomienie miejsc kwarantanny dla osób, które narażone były na zakażenie czynnikiem chorobotwórczym, oraz zabezpieczenie logistyczne przebywających tam osób		wojewoda
27	Wprowadzenie ograniczeń lub zamykanie wytypowanych dróg i obiektów inżynierskich dla ruchu, wyznaczanie objazdów i informowanie użytkowników dróg	Minister Transportu, Budownictwa i Gospodarki Morskiej	Generalny Dyrektor GDDKiA, wojewoda
28	Wprowadzenie dodatkowych procedur kontroli i ostrzegania w przestrzeni powietrznej		Prezes PAŻP

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Lp.	*Moduł zadaniowy (mz)*	*Podmiot wiodący*	*Wykonawca*
29	Przywrócenie działania systemów łączności, odtworzenie systemów łączności na potrzeby kierowania bezpieczeństwem EURO 2012	Minister Administracji i Cyfryzacji	Prezes UKE
30	Przywrócenie zasilania energią elektryczną	Minister Gospodarki, wojewoda	Prezes PSE Operator S.A.
31	Uruchomienie awaryjnego zasilania obiektów ważnych dla EURO 2012		
32	Udział resortu obrony narodowej w zabezpieczeniu Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012	Minister Obrony Narodowej, wojewoda	Szef Centrum Zarządzania Kryzysowego MON
33	Udzielenie pomocy psychologicznej poszkodowanym	wojewoda	wojewoda
34	Zapewnienie transportu zastępczego uczestnikom katastrofy w ruchu drogowym i kolejowym		
35	Zapewnienie awaryjnego oświetlenia ulic dojazdowych do obiektu ważnego dla EURO 2012, funkcjonowania sygnalizacji świetlnej oraz oświetlenia przystanków komunikacji miejskiej		
36	Odtworzenie normalnego funkcjonowania infrastruktury	Minister, wojewoda	podmiot wiodący
37	Zapewnienie polityki informacyjnej		
38	Ostrzeganie i alarmowanie o zagrożeniu uczestników imprez masowych, w tym obywateli państw obcych	MSW, wojewoda	wojewoda

Źródło: Aneks do KPZK 2012

Plik zabezpieczony watermarkiem jawnym i niejawnym: 1475857 3A646 5353

Tabela 11. Przykład zadaniowej siatki bezpieczeństwa – cz. 2. Wykaz wykonawców wraz z realizowanymi modułami dla zagrożenia „Zbiorowe zakłócenie porządku publicznego, w tym zablokowanie przejścia granicznego"

Podmiot wiodący	*Wykonawca*	*Główne zadania*
Minister Spraw Wewnętrznych	Policja Minister Zdrowia Państwowa Straż Pożarna Straż Graniczna Biuro Ochrony Rządu Minister Transportu, Budownictwa i Gospodarki Morskiej /GDDKiA, PKP PLK S.A. MON Służba Celna Prokurator Generalny wojewoda organ administracji samorządowej inne organy, według ustaleń podmiotu wiodącego	8 – Przywrócenie porządku publicznego
		22 – Zapewnienie ratownictwa medycznego poszkodowanym
		18 – Zapewnienie bezpieczeństwa osobom, obiektom i urządzeniom podlegającym ochronie
		27 – Zapewnienie przejezdności wytypowanych dróg, zorganizowanie objazdów i informowanie użytkowników dróg
		18 – Wzmocnienie ochrony jednostek i instytucji oraz obiektów ważnych dla bezpieczeństwa i obronności państwa
		12 – Informowanie właściwych organów zagranicznych o ofiarach – obywatelach państw obcych

Źródło: Aneks do KPZK 2012

Tabela 12. Przykład siatki modułowej – cz. 2. Wykaz wykonawców wraz z realizowanymi modułami dla zagrożenia: „Powódź, katastrofalne zatopienie"

Podmiot wiodący	*Wykonawca*	*Główne zadania*
Minister Spraw Wewnętrznych	Państwowa Straż Pożarna Policja Straż Graniczna Minister Środowiska/KZGW, IMGW Minister Zdrowia Minister Transportu, Budownictwa i Gospodarki Morskiej /GDDKiA, PKP PLK S.A. MON ABW wojewoda organ administracji samorządowej inne organy, wg ustaleń podmiotu wiodącego	38 – Ostrzeganie i alarmowanie o zagrożeniu uczestników imprez masowych, w tym obywateli państw obcych
		3 – Zabezpieczenie obiektów i terenów przed skutkami zalania
		4 – Ewakuacja ludności i zwierząt oraz cennego mienia z zagrożonego rejonu
		22 – Zapewnienie ratownictwa medycznego poszkodowanym
		33 – Udzielenie pomocy psychologicznej poszkodowanym
		7 – Zapewnienie porządku publicznego w miejscu działania służb ratowniczych
		9 – Ochrona pozostawionego mienia

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Podmiot wiodący	*Wykonawca*	*Główne zadania*
		27 – Wprowadzenie ograniczeń lub zamykanie wytypowanych dróg i obiektów inżynierskich dla ruchu, wyznaczanie objazdów i informowanie użytkowników dróg
		12 – Informowanie właściwych organów zagranicznych o ofiarach – obywatelach państw obcych
		Czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze*
		36 – Odtworzenie normalnego funkcjonowania infrastruktury

* Poszczególne moduły opisywały zadania, które uczestnicy mieli wykonać na podstawie poleceń pełnomocnika rządu (patrz tabela 11). Ponieważ prokuratura nie wchodzi w skład administracji rządowej, w siatce zaznaczono jej zadania, jednak bez przypisywania numeru, by nie sugerować, że jest to polecenia do wykonania.

Źródło: Aneks do KPZK 2012

1.8. Podsumowanie rozdziału

Jak wynika w przeprowadzonej analizy, ZK postrzegane początkowo jako system reagowania na sytuacje nadzwyczajne, ze względu na zmiany w otoczeniu prawnym przekształca się w system identyfikowania, oceny i zarządzania ryzykiem. Jednocześnie zapobieganie klęskom żywiołowym (prewencja) staje się równie ważne jak właściwa reakcja na zdarzenie, które już wystąpiło. Zmiana roli i zadań systemu jest również związana z innym, niż jeszcze kilka lat temu, podziałem zadań w ramach bezpieczeństwa narodowego. Zagrożenia hybrydowe powodują, że zaczyna zacierać się granica pomiędzy cywilnym zarządzaniem kryzysowym a zadaniami realizowanymi na rzecz obrony przed agresją militarną. Tym samym problematyka ZK staje się w coraz większym stopniu zagadnieniem wielodyscyplinarnym bazującym zarówno na naukach o bezpieczeństwie, jak i na naukach o zarządzaniu. Należy równocześnie podkreślić, że w obecnym stanie prawnym w ujęciu podmiotowym system skupia się na zagadnieniach związanych z bezpieczeństwem ludzi, mienia oraz środowiska i nie obejmuje takich zagadnień jak niepodzielność terytorialna czy utrzymanie niepodległości. Natomiast w ujęciu przedmiotowym system ma za zadanie uzupełnić możliwości działania organu, którego siły i środki są nieadekwatne w odniesieniu do zagrożenia, które wystąpiło lub może wystąpić w przyszłości. Z tego punktu widzenia zarządzanie kryzysowe jest elementem utrzymania ciągłości działania administracji publicznej w zakresie ochrony ludzi, mienia i środowiska. Jednocześnie rzeczywiste zdarzenia wskazują, że w trakcie działania systemu dochodzi do zakłóceń w jego funkcjonowaniu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rozdział II
Ochrona infrastruktury krytycznej

Poza zarządzaniem sytuacjami kryzysowymi ustawa określa zadania związane z ochroną infrastruktury krytycznej. Jest to związane z możliwością wystąpienia analogicznie niekorzystnej sytuacji nie tylko na skutek działania sił przyrody, ale również w przypadku zakłócenia usług świadczonych przez infrastrukturę techniczną. W tym przypadku ustawa nie skupia się ani na przyczynach zdarzenia, ani na ich bezpośrednich skutkach, lecz na skutkach społecznych dysfunkcji niezbędnych usług (Skomra 2017a).

Włączenie do ustawy zagadnień związanych z niezawodnością techniczną infrastruktury krytycznej oraz odniesienie do usług zapewnianych przez tę infrastrukturę powoduje, że w celu opisu tego obszaru zarządzania kryzysowego należy skorzystać z podejścia procesowego. Badania kolejnego rozdziału będą się więc odnosić do funkcji zarządzania kryzysowego w aspekcie działań zorientowanych procesowo oraz zorientowanych na logistykę. Jednocześnie będą się odnosić do tezy nr 2 (w zakresie wyodrębnienia procesu zarządzania ryzykiem warunkowym i bezwarunkowym) oraz tezy nr 3 (w zakresie związanym z zarządzaniem podatnością.

2.1. Pojęcie infrastruktury krytycznej

Zgodnie z UZK za ochronę IK odpowiada jej operator, zaś administracja publiczna wprowadza standaryzację tej ochrony poprzez nakaz identyfikacji zagrożeń, wraz z oceną związanego z nimi ryzyka. Dodatkowym elementem kontrolnym jest proces zatwierdzania planów ochrony obiektów IK (DzU z 2010 r. nr 83, poz. 542). Z punktu widzenia administracji publicznej jest to więc pewien sposób postępowania z ryzykiem mający na celu uniknięcie wystąpienia sytuacji kryzysowej, choć odmienny od czterofazowego procesu zarządzania sytuacją kryzysową. Podstawowym dokumentem regulującym zasady ochrony IK jest NPOIK. Ingerencja administracji publicznej w sposób zarządzania ryzykiem w obiektach IK wynika z faktu postępującej zależności współczesnego świata od infrastruktury, której funkcjonowanie zapewnia sprawne działanie państwa. Elementy infrastruktury krytycznej (IK) stają się coraz bardziej zależne od siebie, a zniszczenie jednego, przykładowo stanowiącego część krajowego systemu elektroenergetycznego, powoduje perturbacje lub zniszczenie infrastruktury w innych gałęziach

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

gospodarki. Może też wpływać na zapewnienie obywatelom podstawowych usług. Dobrym tego przykładem na gruncie polskim jest awaria sieci przesyłowej, która miała miejsce w Szczecinie w 2008 r. Przerwanie linii energetycznych całkowicie sparaliżowało na kilka dni aglomerację szczecińską oraz dużą część województwa zachodniopomorskiego. W sposób modelowy ukazana tam została współzależność systemów, których działanie jest oparte na energii elektrycznej, oraz tych, które często postrzegane są jako od niej niezależne. Brak zasilania wywołał perturbacje w dziedzinach, w jakich nikt się takiej zależności nie spodziewał. Przykładowo unieruchomienie stacji paliw spowodowało, że po kilku godzinach pojawiły się problemy z utrzymaniem pracy agregatów prądotwórczych w instytucjach, które uważały, że są zabezpieczone przed skutkami takiej sytuacji. Podobnym systemem, którego awaria może spowodować skutki trudne do przewidzenia, są sieci transmisji danych. Na przykład pożar mostu Łazienkowskiego 14 lutego 2015 r. spowodował uszkodzenie linii światłowodowych biegnących w tunelu kablowym pod mostem. Efektem zdarzenia były zaburzenia funkcjonowania sieci telefonicznych i utrudniony dostępu do Internetu w niektórych instytucjach. Przede wszystkim jednak wystąpiły wielogodzinne przerwy w dostępie do baz danych zarządzanych przez administrację rządową.

Proces, który raz zapoczątkowany, w sposób nieunikniony wywołuje kolejne zdarzenia, często nazywany jest „efektem domina", systemy mające kluczowe znaczenie dla funkcjonowania gospodarek i społeczeństw zyskały zaś miano infrastruktury krytycznej. Na świecie ten termin funkcjonuje już od wielu lat. Po raz pierwszy pojawił się w obiegu prawnym w USA w 1998 r., jednak od tego momentu był wielokrotnie modyfikowany. Amerykańska ustawa „Patriot Act" (zastąpiona w 2015 r. przez „Freedom Act") definiowała IK jako „systemy i zasoby fizyczne lub wirtualne tak niezbędne dla Stanów Zjednoczonych, że niesprawność lub zniszczenie tych systemów i zasobów miałoby osłabiający wpływ na bezpieczeństwo, bezpieczeństwo gospodarki narodowej, narodową ochronę zdrowia lub każdą kombinację tych spraw" (*USA Patriot Act*, Section 1016). Na gruncie polskim, zgodnie z UZK (UZK, art. 3 ust. 2), obowiązuje następująca definicja:

Ilekroć mowa o infrastrukturze krytycznej - należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Jednak brak ustawowej definicji IK przed jej przyjęciem nie oznaczał, że taka infrastruktura nie była chroniona (DzU z 2016 r. poz. 1432; DzU z 2003 r. nr 116, poz. 1090 ze zm.) ani że polska administracja nie była z nim zaznajomiona. Polska, jako członek Unii Europejskiej i NATO, brała i bierze czynny udział w pracach organizacji międzynarodowych, gdzie ten termin pojawił się wcześniej niż w UZK.

2.2. Proces wyłaniania IK przy podejściu systemowo-obiektowym

Początkowo ochrona IK miała wynikać z planów sporządzanych przez administrację rządową na szczeblu wojewódzkim i krajowym. Plany miały zawierać m.in. „wykaz obiektów i systemów infrastruktury krytycznej" (UZK, 2007, art. 6 ust. 3 pkt 1)[12], co sugerowało, że wymienione w ustawie systemy w całości są infrastrukturą krytyczną. Szybko się jednak okazało, że przy takiej interpretacji nie można określić, ile jest w kraju obiektów IK, dla ilu z nich opracowano i wdrożono plany ochrony, a tym samym niemożliwym było ustalenie, w jakim stopniu IK jest chroniona. W efekcie poprzez nowelizację ustawy określono precyzyjnie sposób wyłaniania obiektów IK w oparciu o niejawne kryteria będące częścią NPOIK. Nazwa „Program" nie jest tu przypadkowa. Celowo przyjęto, że taki dokument nie powinien być źródłem prawa powszechnie obowiązującego. W przeciwnym wypadku należałoby wprowadzić sankcje za nieprzestrzeganie prawa. Tymczasem karanie ma tę wadę, że wywołuje u wykonawców niechęć do realizacji narzuconych obowiązków (Pyznar 2010).

Aby ustalić, co jest, a co nie jest infrastrukturą krytyczną, opracowano kryteria wyznaczania IK. Cały proces odbywa się w trzech etapach.

Etap pierwszy – kryteria systemowe. W celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK, stosuje się kryteria, właściwe dla danego systemu. W praktyce są to parametry charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi.

Etap drugi – definicja ustawowa. Sprawdzeniu podlega rola, jaką pełni dany obiekt. Polega to na udzieleniu odpowiedzi, czy obiekt, urządzenie, instalacja lub usługa ma kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Upraszczając zapis, etap ten polega

[12] Cytowany art. 6 ust. 3 został uchylony ustawą z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym (DzU nr 131, poz.1076).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

na sprawdzeniu, czy zniszczenie lub zakłócenie funkcjonowania obiektu (wyłonionego w pierwszym etapie) spowodowałoby negatywne skutki dla państwa, obywateli, administracji i innych podmiotów (Skomra 2010).

Etap trzeci – kryteria przekrojowe. W tym etapie ustala się, jakie mogą być potencjalne skutki dysfunkcji obiektu. Kryteria przekrojowe odnoszą się do skutków społecznych zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi i obejmują:

- ofiary w ludziach,
- skutki finansowe,
- konieczność ewakuacji,
- utratę usługi,
- czas odbudowy,
- efekt międzynarodowy,
- unikatowość (rozumianą jako brak możliwości odtworzenia zniszczonego obiektu).

Aby uznać dany obiekt za infrastrukturę krytyczną, potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe. Postępując według powyższego schematu, RCB we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy wymienione w ustawie wytypowało początkowo prawie 700 obiektów, które spełniały ww. kryteria. Z czasem ta ilość spadła do ok. 600. Zmniejszająca się liczba obiektów IK jest spowodowana procesami konsolidacji w systemach łączności i teleinformatycznym. Rozproszone obiekty są obecnie łączone w sieci jednolicie zarządzane pod kątem zapewnienia im bezpieczeństwa. W niektórych przypadkach kilkadziesiąt obiektów zostało obecnie połączonych w jedną sieć funkcjonalną.

W tym miejscu warto zwrócić uwagę na pewien paradoks związany z istnieniem IK. Dla jej właściciela (operatora) infrastruktura powinna przede wszystkim służyć uzyskiwaniu zysku. W razie awarii straty powinny być pokryte ze środków własnych (w ramach bezpieczeństwa finansowego prowadzonej działalności) albo wyrównane poprzez ubezpieczenie (przeniesienie ryzyka na podmiot zewnętrzny). Decyzję o odbudowie powinna poprzedzić analiza kosztów (być może infrastruktury nie opłaca się odbudowywać, a przynajmniej nie w dotychczasowej formie). Z punktu widzenia odbiorcy usługi infrastruktura, a precyzyjniej usługa przez nią świadczona, powinna zostać odtworzona w jak najkrótszym czasie bez względu na koszty. Stąd ostatni etap wyłaniania IK będący w istocie oceną społecznych skutków braku usług realizowanych przez daną IK, jest tak istotny z punktu widzenia administracji publicznej.

2.3. Zarządzanie ryzykiem w ochronie IK

Realizowana w ramach zarządzania kryzysowego ochrona IK została potraktowana bardzo szeroko. Ustawodawca za formę jej ochrony uznał również

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

zapewnienie jej funkcjonalności oraz ciągłości działania, a nie tylko zapewnienie funkcjonowania i szybkiego odtworzenia. Obecne brzmienie terminu ochrony IK (UZK, art. 3 pkt 3) jest efektem implementacji Dyrektywy Rady w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (DzUrz UE L 345/75). Zgodnie z art. 2 dyrektywy ochrona zdefiniowana została jako wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności IK w celu zapobiegania zagrożeniom, różnym rodzajom ryzyka lub słabym punktom oraz ograniczenia i neutralizacji ich skutków. Tę definicję zaimplementowano poprzez nowelizację UZK. W efekcie ustawa określa, że IK ma być chroniona przed wszelkimi zagrożeniami, zarówno spowodowanymi działalnością ludzką (np. atakiem terrorystycznym), jak i przed zagrożeniami naturalnymi czy będącymi skutkiem awarii technicznej[13].

Zazwyczaj ochrona infrastruktury kojarzona jest z ochroną fizyczną. Warto zatem wspomnieć, że zagadnienie to zostało już rozwiązane postanowieniami ustawy o ochronie osób i mienia (UoOOiM) (DzU z 2016 r. poz. 1432). Zgodnie z nią obowiązek stosowania odpowiednich form ochrony obejmuje obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa. Są to m.in. obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej (DzU z 2016 r. poz. 1432, art. 5 ust. 2 pkt 5).

Nałożenie obowiązku ochrony obiektu bądź obszaru wynika z włączenia go do ewidencji obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie. Ewidencję takich miejsc znajdujących się na terenie województwa prowadzi wojewoda. Ma ona charakter poufny. Wykazy obiektów podlegających ochronie sporządzają: prezes Narodowego Banku Polskiego, Krajowa Rada Radiofonii i Telewizji, ministrowie, kierownicy urzędów centralnych i wojewodowie w stosunku do podległych i nadzorowanych służb i podmiotów. Jednak wojewoda, w drodze decyzji administracyjnej, może umieścić w ewidencji obszary, obiekty i urządzenia innych podmiotów niż wymienione w art. 5 ust. 3 ustawy, o ile ich awaria wywoła skutki spełniające przesłanki zawarte w ustawie.

Organem nadzorującym wykonanie obowiązków wynikających z UoOOiM jest komendant wojewódzki policji, który zatwierdza plany ochrony obiektu oraz sprawuje nadzór nad funkcjonowaniem wewnętrznych służb ochrony. Nadzór nad firmami zajmującymi się ochroną fizyczną (specjalistycznymi uzbrojonymi

[13] W kwestii ochrony IK na świecie widoczne są dwa trendy. Pierwszy, w którym ochrona IK nakierowana jest głównie na zagrożenia przed atakami terrorystycznymi, i drugi, w którym ochrona ma na celu przeciwdziałanie wszelkim zagrożeniom. Należy zauważyć, że powoli zmienia się podejście państw w tej kwestii i działania ochrony kierowane są na przeciwdziałanie wszelkim zagrożeniom. Całościowe podejście obejmuje jednocześnie zagrożenia dla IK i zagrożenia powodowane przez dysfunkcję IK. Przykładem kraju, gdzie obowiązuje takie podejście, są Stany Zjednoczone Ameryki.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

formacjami ochronnymi, w skrócie SUFO) sprawuje Komendant Główny Policji, ale realizuje to zadanie poprzez komendanta wojewódzkiego.

Do wyłonienia obiektów i obszarów istotnych dla społeczności lokalnych oraz w celu zapewnienia właściwego poziomu ich ochrony konieczna jest współpraca następujących organów:

- wójta, burmistrza lub prezydenta miasta (ustalenie stopnia ważności obiektu dla społeczności lokalnej, szczególnie dla funkcjonowania aglomeracji miejskich);
- szefem delegatury ABW (uzgadnianie planu ochrony obszarów, obiektów i urządzeń w zakresie zagrożeń o charakterze terrorystycznym);
- wojewody (decyzje administracyjne związane z wykazem obiektów podlegających ochronie);
- komendanta wojewódzkiego policji (zatwierdzanie planu ochrony obiektu, nadzór nad funkcjonowaniem służb ochrony).

Niekiedy utrzymywanie pełnej ochrony fizycznej obiektu jest ekonomicznie nieuzasadnione. W takim przypadku w planach ochrony obiektów można zawrzeć różne formy ochrony stosowane w zależności od stopnia zagrożenia. Źródłem informacji o podwyższonym zagrożeniu mogą być zarówno polecenia wydawane przez szefa ABW (DzU z 2016 r. poz. 904, art. 4 ust. 3), jak wykaz zadań wynikających z wprowadzenia jednego ze stopni alarmowych (DzU z 2016 r. poz. 904, art. 15–17).

Jednak ochrona fizyczna to tylko jeden z elementów kompleksowej ochrony IK. Działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia IK przez:

- zmniejszenie prawdopodobieństwa wystąpienia zagrożenia;
- zmniejszanie podatności;
- minimalizowanie skutków wystąpienia zagrożenia.

Na te działania składają się:

1) zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
2) zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

4) zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
5) zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

Zastosowanie konkretnych środków zapewnienia bezpieczeństwa powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK (NPOIK, s. 31–32). Zgodnie z UZK ochrona IK spoczywa przede wszystkim na właścicielach oraz posiadaczach samoistnych i zależnych obiektów, instalacji lub urządzeń IK (UZK, art. 6). Zasadnicze zadania ciążące na operatorze to wskazanie osoby do kontaktów z administracją publiczną oraz opracowanie planu ochrony IK. Plany, zarówno już posiadane, jak i opracowane na nowo, zatwierdzane są przez dyrektora RCB. Plany podlegają aktualizacji w zależności od potrzeb, ale nie rzadziej niż raz na dwa lata. Mając na uwadze, że nie wszyscy właściciele oraz posiadacze IK mogą posiadać odpowiednie poświadczenia i warunki przetwarzania informacji niejawnych, do planów stosować można przepisy o ochronie informacji niejawnych albo o ochronie tajemnicy przedsiębiorstwa.

Ponieważ administracja publiczna, poza nielicznymi wyjątkami, nie ma możliwości prowadzenia kontroli w podmiotach gospodarczych, proces zatwierdzania planu jest podstawową formą działań mających na celu zmniejszenie poziomu ryzyka w obiektach IK. Dopiero po wprowadzeniu 2 lub wyższego stopnia alarmowego administracja aktywnie włącza się do działań mających chronić obiekty IK. I tak m.in. szef ABW, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, może wydać Policji zalecenie szczególnego zabezpieczenia poszczególnych obiektów uwzględniające rodzaj zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym (DzU z 2016 r. poz. 904, art. 12 ust. 2).

Jednocześnie jednak administracja podejmuje działania mające ochronić ludność przed skutkami dysfunkcji IK. W planach zarządzania kryzysowego, zarówno na szczeblu gminnym, powiatowym, wojewódzkim, jak i krajowym, umieszcza się wykaz IK na danym terenie oraz uwzględnia się charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dotyczących IK. Dodatkowo w planach określa priorytety w zakresie ochrony oraz odtwarzania IK. W efekcie administracja publiczna planuje zarówno działania na rzecz ochrony obiektu IK, jak i działania na rzecz ludności cywilnej, o ile dojdzie do dysfunkcji systemu IK.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

2.4. Podsumowanie rozdziału

Na bazie podejścia organizacyjno-prawnego nie można określić wszystkich zależności, jakie występują pomiędzy administracją publiczną, operatorami IK i celami działania zarządzania kryzysowego. Dopiero podejście procesowe pozwala zauważyć, że istnieją dwa powiązane ze sobą procesy, tj. proces zarządzania ryzykiem nakierowany na utrzymanie ciągłości IK (z punktu widzenia administracji publicznej jest to ryzyko bezwarunkowe) oraz proces zarządzania ryzykiem zakłóceń spowodowanych dysfunkcją IK (ryzyko warunkowe). Pierwszy jest domeną operatora IK i poza zatwierdzaniem planów administracja publiczna nie ma bezpośredniego wpływu na zarządzanie tym ryzykiem (wyjątkiem jest sytuacja, w której sama administracja jest właścicielem takiej infrastruktury). Drugi proces (warunkowany wystąpieniem zakłócenia w funkcjonowaniu IK) jest związany z ochroną ludności przed skutkami braku usług zapewnianych przez tę infrastrukturę. Ten obszar jest domeną administracji publicznej i wchodzi w zakres zarządzania kryzysowego, a precyzyjnie zarządzania sytuacją kryzysową.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rozdział III
System zarządzania kryzysowego w ujęciu teoretycznym

Kolejna część badań jest poświęcona zależnościom, jakie występują pomiędzy zarządzaniem bezpieczeństwem narodowym a zarządzaniem kryzysowym. Ich celem jest określenie obszaru zadaniowego przypisanego zarządzaniu kryzysowemu w ramach modelu kierowania bezpieczeństwem narodowym. Proces badawczy odnosi się do tezy nr 1 (w zakresie wydzielenia obszaru zarządzania kryzysowego) i bazuje na możliwości wykorzystania klasycznej kwalifikacji ryzyka. Klasyczna kwalifikacja ryzyka pozwala podzielić działania zapobiegawcze na trzy kategorie:

- ukierunkowane na zagrożenie,
- ukierunkowane na podatności,
- ukierunkowane na skutki.

Aby ją zastosować, wykorzystywane jest podejście procesowe.

Ważnym elementem jest dyskusja pojęcia „kryzys" i „sytuacja kryzysowa" w rozumieniu nauk o bezpieczeństwie oraz nauk o zarządzaniu. Jej celem jest ustalenie, które podstawy naukowe i przy jakich uwarunkowaniach są właściwe do prowadzenia rozważań prowadzących do ujawnienia powiązań ryzyka bezwarunkowego i warunkowego z ryzykiem operacyjnym. Dodatkowym elementem rozważań jest wskazanie obszaru nauki właściwego dla zarządzania ryzykiem realizowanego przez administrację publiczną. Brane są pod uwagę trzy możliwości:

- logistyka biznesu (cywilna),
- logistyka społeczna,
- logistyka wojskowa (militarna).

3.1. Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego

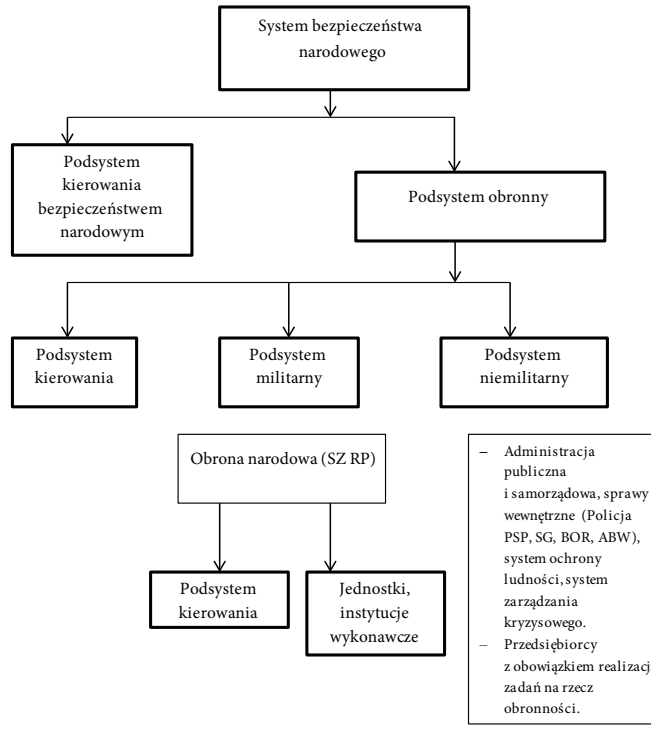
Jak już wspomniano we wprowadzeniu, zarządzanie kryzysowe w rozumieniu ustawy to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym. Jednocześnie ustawa nie precyzuje ani dlaczego jest to element kierowania bezpieczeństwem narodowym, ani w jakim zakresie. Literatura przedmiotu inaczej lokuje zarządzanie kryzysowe. W ujęciu systemowym (Marczak 2008) bezpieczeństwo narodowe to całokształt

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

przygotowania i organizacji państwa do ciągłego budowania i utrzymywania bezpieczeństwa narodowego obejmujący następujące podstawowe elementy:

- prawne podstawy bezpieczeństwa;
- politykę i strategię bezpieczeństwa;
- cywilną i wojskową organizację ochrony i obrony narodowej;
- infrastrukturę bezpieczeństwa;
- sojusze i współpracę międzynarodową w zakresie bezpieczeństwa.

Z tego punktu widzenia system obronny wraz ze swoimi podsystemami wchodzi w skład systemu bezpieczeństwa narodowego i jednocześnie jest jego podsystemem. Tę tezę przedstawiono na schemacie nr 6.


System bezpieczeństwa narodowego
Podsystem kierowania bezpieczeństwem narodowym
Podsystem obronny
Podsystem kierowania
Podsystem militarny
Podsystem niemilitarny
Obrona narodowa (SZ RP)
Podsystem kierowania
Jednostki, instytucje wykonawcze
– Administracja publiczna i samorządowa, sprawy wewnętrzne (Policja PSP, SG, BOR, ABW), system ochrony ludności, system zarządzania kryzysowego.
– Przedsiębiorcy z obowiązkiem realizacji zadań na rzecz obronności.

Schemat 6. System obronny w systemie bezpieczeństwa narodowego
Źródło: Majchrzak 2011, s. 54

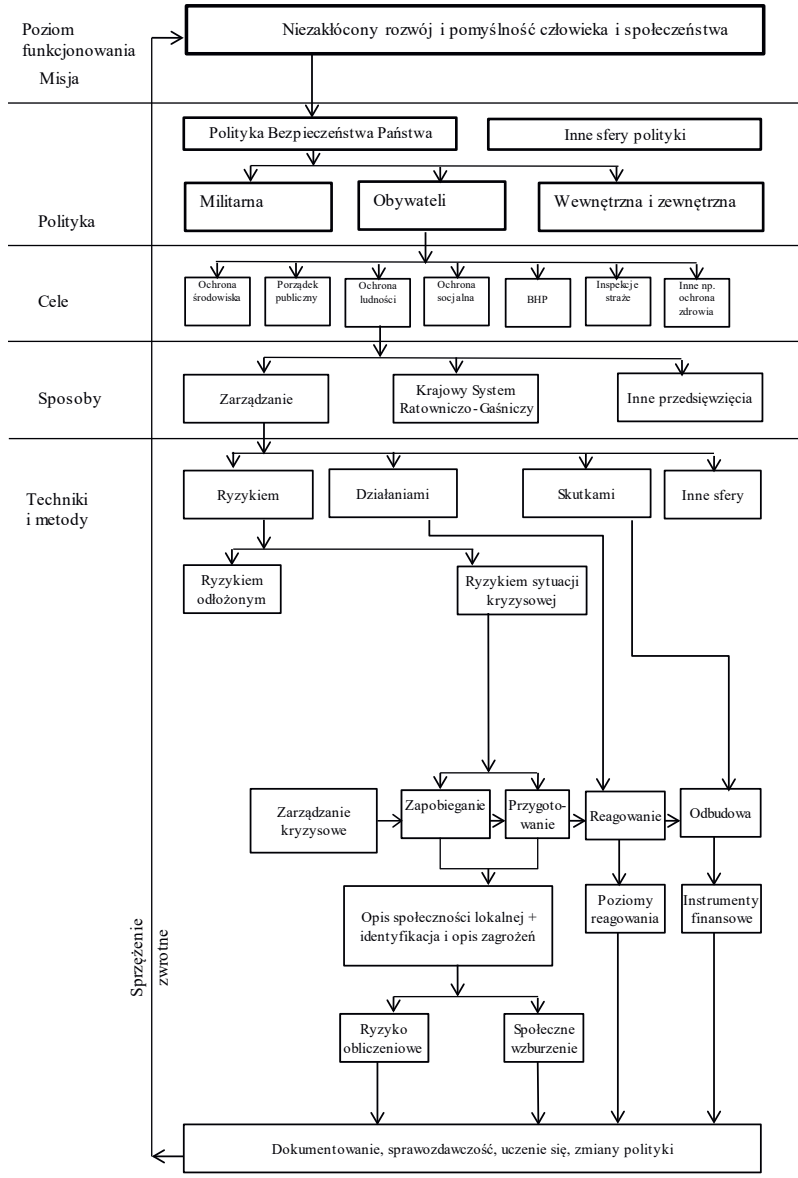
W tym ujęciu można wyróżnić następujące cechy zarządzania kryzysowego (Majchrzak 2001):

- jest ono dziedziną związaną z bezpieczeństwem narodowym;
- jest częścią teorii i praktyki zarządzania organizacją w ogóle;
- wiąże się z procesami zarządzania ryzykiem;
- jest działaniem w czasie napiętych pod względem czasowym sytuacji, gdzie zaniechanie działania może doprowadzić do kryzysu;

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

– jest działaniem realizowanym na skutek przekroczenia akceptowalnego poziomu zagrożeń;
– jest działaniem w warunkach niedoboru sił i środków.

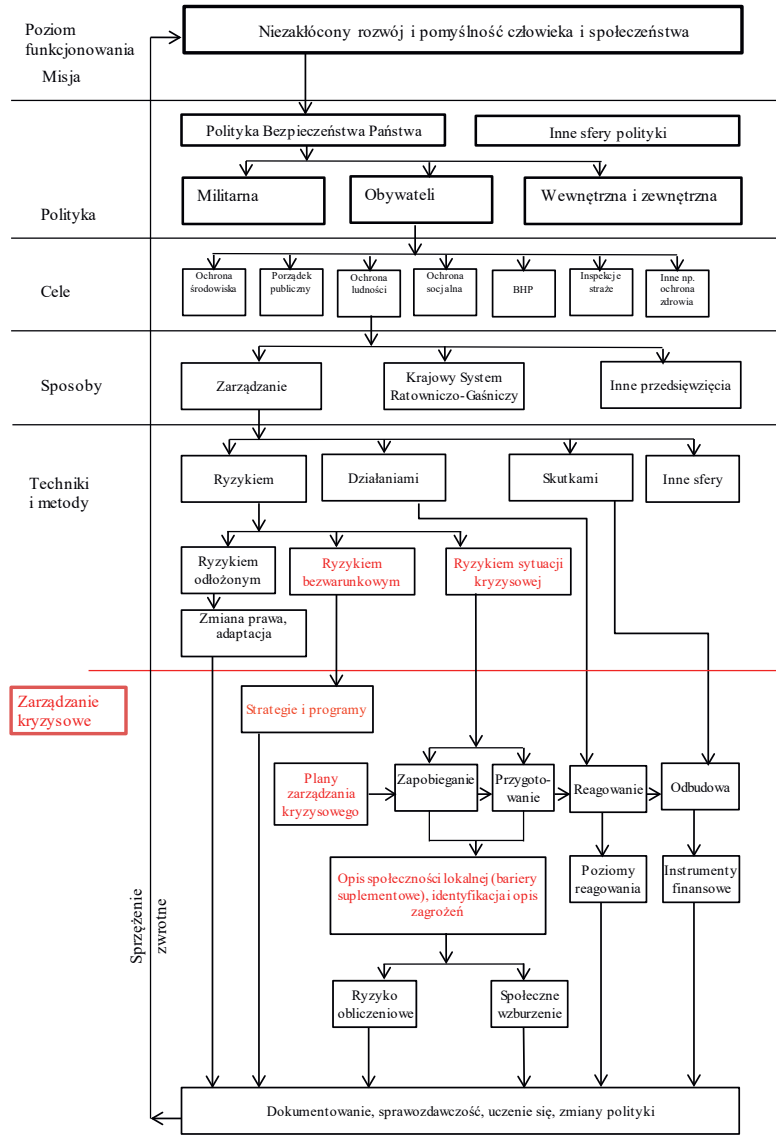
Biorąc pod uwagę funkcje realizowane przez państwo (misja, polityka, cele, sposoby, techniki i metody), umocowanie zarządzania kryzysowego w strukturze bezpieczeństwa przedstawiono na schemacie nr 7.



Schemat 7. Model funkcjonalno-strukturalny systemu bezpieczeństwa
Źródło: Wolanin 2005, s. 364

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zgodnie z przedstawionym schematem zarządzanie kryzysowe jest sytuowane w obszarze zarządzania ryzykiem innym niż ryzyko odłożone. Uwzględniając dotychczasowy proces badawczy, przedstawiony schemat można uzupełnić o ryzyka warunkowe i bezwarunkowe, wskazać sposób postępowania w obu przypadkach i ostatecznie określić obszar zarządzania kryzysowego. Zmodyfikowany model przedstawiono na schemacie nr 8.



Schemat 8. Model funkcjonalno-strukturalnego systemu bezpieczeństwa z uwzględnieniem ryzyka warunkowego i bezwarunkowego

Źródło: opracowanie własne na podstawie: Wolanin 2005, s. 364

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zgodnie z przedstawionym schematem na zarządzanie kryzysowe składa się zarządzanie ryzykiem bezwarunkowym oraz ryzykiem warunkowych (ryzykiem wystąpienia sytuacji kryzysowej). Zależności pomiędzy ryzykiem bezwarunkowym a ryzykiem wystąpienia sytuacji kryzysowej wymagają szerszego omówienia. Aby je wyjaśnić na przykładzie, można się posłużyć następującym stwierdzeniem hipotetycznym: „W związku z istniejącym ryzykiem powodziowym, o ile dojdzie do jego zmaterializowania się (wystąpi zdarzenie krytyczne w postaci powodzi), to ze względu na możliwą nieadekwatność posiadanych sił i środków (zależną od wielkości powodzi i posiadanych zasobów) istnieje ryzyko wystąpienia sytuacji kryzysowej". W powyższym stwierdzeniu mamy dwa rodzaje ryzyka, z których pierwsze jest ryzykiem bezwarunkowym, natomiast drugie może się zmaterializować pod warunkiem wystąpienia zdarzenia krytycznego (powodzi). Ryzyko powodzi jest więc ryzykiem bezwarunkowym, będącym kombinacją prawdopodobieństwa wystąpienia powodzi i spodziewanych strat, gdzie powódź jest losowo występującym zagrożeniem naturalnym. Ryzyko wystąpienia sytuacji kryzysowej jest ryzykiem warunkowym uzależnionym od wystąpienia zdarzenia krytycznego (powodzi) i jest związane z zawodnością barier suplementowych i systemowych (Skomra 2015). Pojęcie „ryzyko warunkowe" nie jest stosowane powszechnie w literaturze przedmiotu. Używa się natomiast pojęcia „prawdopodobieństwo warunkowe" o ile jedno zdarzenie zachodzi z pewnym prawdopodobieństwem pod warunkiem, że wcześniej zaszło inne zdarzenie (Chung 2006). W zarządzaniu ryzykiem znane jest też pojęcie „zdarzenie krytyczne" (Abgarowicz 2015), które warunkuje dalszy ciąg zdarzeń. Ten dalszy ciąg zdarzeń jest opisywany w postaci „funkcji warunkowych" (DeWolf 2003; Wolanin 2005). Dla ryzyk powiązanych ze sobą (skorelowanych) używa się również określenia „ryzyko zależne" (Denuit, Dhaene, Goovaerts, Kaas 2005), jednak wzajemna zależność różnych rodzajów ryzyka nie musi być warunkowana wystąpieniem zdarzenia krytycznego. Z tych względów, w dalszej części opracowania, w celu zachowania jednoznaczności pojęć konsekwentnie będzie używane określenie ryzyko bezwarunkowe (niepoprzedzone zdarzeniem krytycznym) i warunkowe (poprzedzone zdarzeniem krytycznym).

W myśl przedstawionego schematu zarządzanie kryzysowe nie obejmuje zarządzania ryzykiem odłożonym, które to ryzyko wynika z działalności człowieka, a negatywne skutki tego oddziaływania na ludzi, otoczenie cywilizacyjne i środowisko naturalne są odłożone w czasie. Przykładem takiego ryzyka są zmiany demograficzne, zmiany klimatu czy długotrwałe zanieczyszczenie środowiska (Wolanin 2005). W przypadku ryzyka odłożonego nie występuje faza przygotowania i reagowania. Natomiast, poprzez właściwą politykę, istnieje możliwość zapobiegania możliwości wystąpienia ryzyka. Przykładowo właściwa polityka społeczna może zapobiegać niekorzystnym zmianom demograficznym. Istnieje również możliwość łagodzenia skutków poprzez proces adaptacji (np. adaptacja do zmian klimatu). Nie ma jednak możliwości planowego reagowania na wystąpienie sytuacji kryzysowej. Różnice w podejściu do zarządzania ryzykiem bezwarunkowym i warunkowym przestawiono w tabeli nr 13.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 13. Porównanie procesów: zarządzania, zarządzania ryzykiem i zarządzania ryzykiem sytuacji kryzysowych

Zarządzanie	*Zarządzanie ryzykiem bezwarunkowym*	*Zarządzanie ryzykiem warunkowym (ryzykiem sytuacji kryzysowych)*
Określenie problemu	Opis systemu; przyjęcie założeń: strategicznych, organizacyjnych i zarządzania ryzykiem; opracowanie kryteriów oceny zagrożenia; decyzje dotyczące struktury	Opis systemu definiowanie problemu przyjęcie zakresu zarządzania ryzykiem sytuacji kryzysowych opracowanie kryteriów oceny ryzyka wystąpienia zdarzenia niekorzystnego
Badania	Identyfikacja ryzyka Co może się wydarzyć? W jaki sposób to się może wydarzyć?	Identyfikacja ryzyka identyfikacja i opis źródeł ryzyka opis podatności opis ryzyka
Analiza	Analiza ryzyka określenie istniejącej kontroli; określenie częstotliwości i skutków; szacowanie poziomu ryzyka	Analiza ryzyka – określenie częstotliwości i skutków;
Podejmowanie decyzji	Ocena ryzyka porównanie kryteriów; ustalenie hierarchii ryzyka decyzja o akceptacji ryzyka	Ocena ryzyka porównanie kryteriów; ustalenie hierarchii ryzyka decyzja o akceptacji ryzyka
	Ograniczanie ryzyka identyfikacja opcji redukcji ryzyka ocena opcji redukcji ryzyka wybór opcji redukcji ryzyka	Ograniczanie ryzyka identyfikacja opcji redukcji ryzyka ocena opcji redukcji ryzyka wybór opcji redukcji ryzyka
Wdrażanie	Przygotowanie planów redukcji ryzyka Wdrażanie	Plan i wdrażanie redukcji ryzyka
Obserwacja	Obserwacja	Obserwacja
Łączność i konsultacje	Łączność i konsultacje	Łączność i konsultacje

Źródło: Australijska Agencja ds. Sytuacji Nadzwyczajnych (EMA 1999), w ślad za: Wolanin 2005, s. 166

3.2. Zarządzanie społecznymi skutkami zmaterializowania się ryzyka

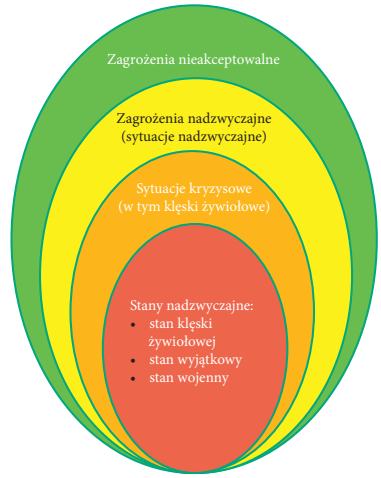
W ujęciu podmiotowym (oddziaływanie na ludzi, ich mienie, środowiska oraz infrastrukturę krytyczną) zarządzanie kryzysowe należy wiązać domenami bezpieczeństwa. J. Wolanin (Wolanin 2005) wskazuje na cztery takie domeny. Podstawową jest domena bezpieczeństwa indywidualnego, która charakteryzuje się tym, że służby publiczne praktycznie nie mają wpływu na decyzje podejmowane indywidualnie

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

przez każdego obywatela. Nie oznacza to, że administracja nie może oddziaływać na postawy ludzi poprzez edukację, która pozwala nauczyć obywatela bezpiecznych zachowań. Również na obszar relacji mikrospołecznych (rodziny, sąsiadów, znajomych) władze nie mają bezpośredniego wpływu, choć poprzez wspieranie rozwoju więzi społecznych mogą długofalowo wzmacniać zdolność społeczności lokalnej do uporania się z potencjalną katastrofą. Dwie domeny, które stanowią zasadniczy obszar działania władzy publicznej, a więc również zarządzania kryzysowego, to domena bezpieczeństwa lokalnego i państwowego (Wolanin 2005). Na tych poziomach władze mogą przygotowywać zasoby, wyposażać służby reagowania kryzysowego i zapewnić infrastrukturę poprawiającą bezpieczeństwo obywateli (np. chodniki dla pieszych, przejścia dla pieszych z sygnalizacją świetlną itp.).

Analogicznym podziałem obszaru oddziaływania poprzez zdefiniowanie domen bezpieczeństwa posługuje się logistyka (Szymonik, Bielecki 2015). Wskazuje to powiązanie zarządzania kryzysowego z logistyką poprzez wspólne zadanie, jakim jest zapewnienie i utrzymanie dostępności zasobów niezbędnych w sytuacjach kryzysowych.

W ujęciu przedmiotowym, gdy przedmiotem badań jest sama administracja publiczna i sprawność jej działania w obliczu sytuacji trudnych (kryzysowych), zarządzanie kryzysowe jest systemem uzupełniającym w przypadku, gdy skala, charakter lub rodzaj zagrożenia doprowadza lub może doprowadzić do znacznego ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków. Rodzaje takich sytuacji wraz z umiejscowieniem sytuacji kryzysowej przedstawiono na schemacie nr 9.



Schemat 9. Zależności pomiędzy sytuacjami kryzysowymi a innymi sytuacjami wynikającymi z występujących zagrożeń

Użyte na schemacie określenia oznaczają:

– Zagrożenia nieakceptowalne – są to nieakceptowalne społecznie zagrożenia o typowym charakterze i zasięgu terytorialnym, wymagające podjęcia autonomicznych

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

działań przez służby, inspekcje i straże przy rutynowym wsparciu innych służb i organów w oparciu o wspólne plany i procedury.

– Zagrożenia nadzwyczajne – są to nieakceptowalne społecznie zagrożenia dla życia, zdrowia bądź środowiska, które ze względu na swój charakter bądź zasięg wykraczają poza ramy działań rutynowych poszczególnych służb, inspekcji bądź straży.
– Sytuacja kryzysowa to szczególny przypadek sytuacji nadzwyczajnej, w trakcie której doszło do znacznego ograniczenia działalności właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił, środków bądź kompetencji.
– Stan nadzwyczajny to pojawienie się w państwie sytuacji kryzysowej, do której rozwiązania zwykłe środki konstytucyjne są niewystarczające (efektem wprowadzenia stanu nadzwyczajnego może być koncentracja władzy w rękach prezydenta i rządu, ograniczenie praw i wolności obywateli, zmiany w strukturze i zasadach funkcjonowania organów państwowych oraz zmiany w systemie stanowienia prawa.

Źródło: Skomra 2016, s. 44

W tym ujęciu zarządzanie kryzysowe wiąże się z działaniem organizatorskim (koordynacja) i zapewnieniem dostępności do zasobów osobowych, materialnych, informacyjnych i finansowych (ustawa używa określenia „siły i środki"). Celem realizowanym w ramach zarządzania kryzysowego jest utrzymanie ciągłości działania organu, którego siły i środki okazały się nieadekwatne do występującego zagrożenia. To podejście jest zbieżne z celami, jakimi kieruje się logistyka społeczna (Szołtysek 2014).

Rolę zarządzania kryzysowego z perspektywy wszystkich trzech omawianych ujęć przedstawiono w tabeli nr 14.

Tabela 14. Rola zarządzania kryzysowego

Badany obszar	*Cel działania*	*Realizowane działania*
Bezpieczeństwo narodowe	Zarządzanie ryzykiem wystąpienia sytuacji kryzysowej	Monitorowanie zagrożeń dla bezpieczeństwa narodowego, ocena ryzyk związanych z tymi zagrożeniami, planowanie zasobów, testowanie
Administracja publiczna	Element utrzymania ciągłości działania administracji publicznej pod presją zagrożenia	Działalność organizatorska (koordynacja) oraz zapewnienie dostępu do zasobów osobowych, materialnych, informacyjnych i finansowych[1]
Ludność, mienie i środowisko oraz ochrona infrastruktury krytycznej	Element domeny lokalnej i państwowej	Standaryzacja postępowania z ryzykiem dysfunkcji infrastruktury krytycznej. Budowanie świadomości ryzyka i odporności na ryzyko

Źródło: opracowanie własne

[14] Ustawa o zarządzaniu kryzysowym używa określenia „siły i środki". Co wchodzi w zakres tak określanych zasobów, można wywnioskować z zawartości planów zarządzania kryzysowego.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

3.3. Zarządzanie kryzysowe w naukach o bezpieczeństwie i w naukach o zarządzaniu

Definicje, pojęcia i fazy działania zawarte w ustawie o zarządzaniu kryzysowym zostały oparte na definicjach i podejściu zaproponowanym przez teorię kryzysu w ramach nauk o bezpieczeństwie (Wróblewski 1996). Natomiast biorąc pod uwagę konieczność zarządzania ryzykiem w ramach zarządzania kryzysowego, Zawiła-Niedźwiecki lokuje zarządzanie kryzysowe w obszarze logistyki społecznej w ramach nauk o zarządzaniu (Zawiła-Niedźwiecki 2015). Równocześnie wskazuje, że obszar ten nie jest dostatecznie przebadany, zaś poszczególne elementy wchodzące w obszar zarządzania kryzysowego są w zainteresowaniu wielu dziedzin nauki.

W ramach logistyki społecznej zakłada się, że istnieją pewne usługi np. związane z ratowaniem zagrożonego życia i zapewnieniem bezpieczeństwa (publicznego oraz w przestrzeni publicznej), które nie są realizowane z potrzeby zysku (Szołtysek 2014). Inaczej podeszli do tego zagadnienia twórcy podziału logistyki na wojskową i kryzysową. Według tej koncepcji głównym celem działania logistyki cywilnej jest maksymalizacja zysku przedsiębiorstwa, zaś logistyki kryzysowej jest zaspokojenie elementarnych potrzeb logistycznych ludności. W tym drugim przypadku rachunek ekonomiczny ma znaczenie trzeciorzędne (Nowak 2009). Oba te podejścia można połączyć poprzez zdefiniowanie logistyki cywilnej (biznesu), społecznej i wojskowej (militarnej). Porównanie poszczególnych rodzajów logistyki przedstawiono w tabeli nr 15.

Tabela 15. Komparystyka czystych typów logistyki

	Logistyka biznesu	*Logistyka społeczna*	*Logistyka militarna*
Publiczny dostęp do informacji	ograniczony	otwarty	wyłączony
Publiczny dostęp do procesu	ograniczony	otwarty	wyłączony
Właściciel procesu	podmiot gospodarczy	społeczeństwo/ społeczność lokalna/ grupa ludzi	państwo bądź organizacja aspirująca do spełniania funkcji państwa i monopolizowania aparatu przemocy
Zarządca procesu	organ podmiotu gospodarczego	instytucja władzy publicznej, organizacja społeczna bądź osoby fizyczne	instytucja władzy państwowej, kierownictwo służb
Bezpośredni odbiorca procesu	nabywca/konsument	użytkownik/członek wspólnoty/obywatel	każdy zagrożony bądź uwikłany w działania odpowiednich służb

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

	Logistyka biznesu	*Logistyka społeczna*	*Logistyka militarna*
Ostateczny odbiorca procesu	konsument	społeczeństwo	społeczeństwo/ naród/ grupa etniczna
Pryzmat podejmowanych decyzji zarządczych	ekonomiczna	humanitarna	organizacyjna
Priorytet	zysk	jakość życia	bezpieczeństwo
Dominujące przesłanki podejmowania decyzji zarządczych	ekonomiczność i korzystność	skuteczność i korzystność	skuteczność
Przedmiot	przepływy materialne (osobowe i rzeczowe) oraz towarzyszące informacje		
Cel	nadanie walorów czasoprzestrzennych (i uzupełniających) przedmiotom przepływu		

Źródło: Szołtysek, Twaróg 2013, s. 25; na podstawie: Kołodziejczyk, Szołtysek 2009, s. 23

W celu stwierdzenia, w której z dziedzin nauki należy ulokować zarządzanie kryzysowe, można porównać pojęcia charakteryzujące to zarządzanie w ujęciu nauk o bezpieczeństwie i nauk o zarządzaniu.

Zasadniczymi pojęciami stosowanymi w badanym systemie są „kryzys", „sytuacja kryzysowa" i „zarządzanie kryzysowe". W obu wymienionych obszarach nauki rozumienie tych terminów jest diametralnie różne.

Kryzys w sensie przedmiotowym to zerwanie istniejącego układu, polegające na zmianie jego struktury lub funkcji albo obu tych elementów łącznie (Wróblewski 1996, s. 9).

Kryzysem będziemy nazywali kulminacyjną fazę eskalacji zagrożenia, często całkowitą utratę kontroli nad zaistniałą sytuacją, w której następuje przełom (punkt zwrotny) jakiegoś procesu, w wyniku którego dany podmiot może ulec likwidacji, destrukcji lub (uzyskać szansę – przyp. autora) powrotu do normalności, a nawet rozwoju (Marszałek, Sobolewski, Majchrzak 2012, s. 31)**.**

To samo pojęcie w naukach o zarządzaniu jest prezentowane w innym kontekście:

Kryzys to stan, który zagraża przetrwaniu firmy, realizacji jej celów, ogranicza czas dostępny na podjęcie działań zaradczych i zaskakuje decydentów swoim pojawieniem się, stwarzając w ten sposób warunki silnej presji (Herman 1963).

Kryzys – odbiegająca od normy i niestabilna sytuacja zagrażająca celom strategicznym, reputacji organizacji lub jej żywotności (BS 11200:2014, s. 2).

Porównanie obu podejść do pojęcia „kryzys" przedstawiono w tabeli nr 16.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 16. Porównanie definicji kryzysu w różnych ujęciach

	Czas trwania	*Możliwość zarządzania*
Nauki o bezpieczeństwie	Przełom, punkt zwrotny, moment	Utrata możliwości zarządzania sytuacją
Nauki o zarządzaniu	Stan, faza, okres, sytuacja	Wymagane zarządzanie pod presją czasu

Źródło: opracowanie własne

Analogicznie występują rozbieżności w definiowaniu pojęcia „sytuacja kryzysowa", które jest interpretowane następująco:

Sytuacja kryzysowa – zespół okoliczności zewnętrznych i wewnętrznych, w jakich znajduje się dany podmiot (układ, organizacja, system), wpływających na jego funkcjonowanie w taki sposób, iż zaczyna się w nim i jest kontynuowany proces zmienny, w rezultacie czego dochodzi do zachwiania równowagi i utraty możliwości kontroli nad przebiegiem wydarzeń albo eskalacji zagrożenia jego interesów (Gryz, Kitler 2007, s. 22).

Sytuacja kryzysowa organizacji – taki jej stan, będący wynikiem kształtowania się pewnych niekorzystnych zjawisk w czasie, który nie rodzi bezpośredniego zagrożenia egzystencji organizacji, ale oznacza niezadowalającą ocenę jej działalności z punktu widzenia zmian zachodzących w otoczeniu i/lub w stosunku do stanów (ocen) wzorcowych (Kral, Zabłocka-Kluczka 2003, s. 20).

Porównanie pojęcia „sytuacja kryzysowa" w ujęciu nauk o bezpieczeństwie i nauk o zarządzaniu przedstawiono w tabeli nr 17.

Tabela 17. Porównanie pojęcia „sytuacja kryzysowa" w różnych ujęciach

	Zasadnicze elementy definicji	*Możliwości zarządzania*
Nauki o bezpieczeństwie	Proces prowadzący do utraty kontroli nad sytuacją (faza poprzedzająca kryzys)	Wymaga nadzwyczajnych działań (nadzwyczajne rozwiązania prawne i organizacyjne np. wprowadzenie stanu nadzwyczajnego)
Nauki o zarządzaniu	Niezadowalający stan organizacji	Wymagane wdrożenie procesu zarządzania pod presją czasu

Źródło: opracowanie własne

Jednak najbardziej istotne są różnice w interpretowaniu pojęcia „zarządzanie kryzysowe". W myśl nauk o bezpieczeństwie jego definicja może wyglądać następująco:

Zarządzanie kryzysowe w dziedzinie bezpieczeństwa to działanie przy użyciu różnych środków (m.in. dyplomatycznych, specjalnych, ekonomicznych, militarnych, normatywnych) i zasobów (ludzkich, finansowych, materialnych i intelektualnych), podejmowane w przewidywaniu lub w razie wystąpienia sytuacji trudnych, krytycznych, jednym słowem zakłócających funkcjonowanie

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

środowiska międzynarodowego i naruszających proces rozwoju gospodarczego i społecznego, lecz także prawa człowieka, porządek publiczny i ład międzynarodowy (wewnętrzny), równowagę przyrodniczą itd." (Kitler 2011, s. 18).

To samo pojęcie w normie pt. „Zarządzanie kryzysowe – wytyczne i dobre praktyki" zdefiniowano następująco:

Zarządzanie kryzysowe to rozwijanie i wykorzystanie zdolności organizacji do radzenia sobie z kryzysem (BS 11200: 2014, s. 2).

Porównanie pojęcia „zarządzanie kryzysowe" w ujęciu nauk o bezpieczeństwie i nauk o zarządzaniu przedstawiono w tabeli nr 18.

Tabela 18. Porównanie pojęcia „kryzys" w różnych ujęciach

	Zasadnicze elementy definicji	*Podejście do zarządzania*
Nauki o bezpieczeństwie	Działania podejmowane w przewidywaniu lub w razie wystąpienia sytuacji trudnych, krytycznych.	Dyskretne (nieciągłe)
Nauki o zarządzaniu	Stałe budowanie i utrzymywanie zdolności organizacji do radzenia sobie z kryzysem	Procesowe

Źródło: opracowanie własne

Jak widać z przeprowadzonej analizy, zarządzanie kryzysowe w ujęciu nauk o bezpieczeństwie łączy się z podejmowaniem incydentalnie nadzwyczajnych działań w sytuacji zagrożenia. Dla nauk o zarządzaniu jest to realizowany stale proces osiągania i utrzymania zdolności organizacji (państwa, systemu) do radzenia sobie z przypadkami, gdy stan organizacji staje się „niezadowalający". W praktyce o tym czy poprawne jest podejście stosowane w naukach o bezpieczeństwie, czy wynikające z nauk o zarządzaniu, decyduje charakter realizowanych zadań. Dla zadań realizowanych incydentalnie opartych na działaniach w sferze politycznej, właściwym jest podejście stosowane w naukach o bezpieczeństwie. W przypadku zadań o charakterze ciągłym właściwe jest podejście procesowe i pojęcia wynikające z nauk o zarządzaniu. Przy tym podejściu, poza realizacją celów organizacji, należy uwzględniać zagadnienia wiążące się z zarządzaniem ryzykiem operacyjnym. Zarządzaniem, które skupia się na zagadnieniach związanych z działaniem organizatorskim i dostępnością do zasobów osobowych, materialnych, informacyjnych i finansowych[15].

Jednocześnie należy odnotować, że do korzystania z dorobku nauk o zarządzaniu przy zarządzaniu ryzykiem zachęca szereg dokumentów UE. Przykładowo dyrektywa unijna w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych (DzUrz UE L 194/1, dalej NIS), która powołuje się na zarządzanie ryzykiem operacyjnym oraz zakłada podejście

[15] Ustawa o zarządzaniu kryzysowym używa określenia „siły i środki". Co wchodzi w zakres tak określanych zasobów, można wywnioskować z zawartości planów zarządzania kryzysowego.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

procesowe w zapewnieniu usług świadczonych przez administrację publiczną. Z kolei dokument Komisji Europejskiej pt. „Wytyczne oceny zdolności zarządzania ryzykiem" (DzUrz UE 2015/C 261/03) powołuje się na normę Zarządzanie ryzykiem – Zasady i wytyczne (PN-ISO 31000:2012) oraz model doskonałości EFQM. Model EFQM obejmuje osiem zasad doskonałości. Jedną z nich jest zarządzanie poprzez procesy (Kosieradzka, Zawiła-Niedźwiecki 2016). Podejście procesowe przy świadczeniu usług na rzecz ludności pojawia się również w krajowych dokumentach normatywnych, choć na razie dotyczy to tylko obszaru usług związanych z infrastrukturą telekomunikacyjną (DzU z 2016 r. poz. 113).

3.4. Podsumowanie rozdziału

Korzystając z podejścia procesowego, można zdefiniować domenę zarządzania kryzysowego jako związaną z zarządzaniem ryzykiem odłożonym, ryzykiem bezwarunkowym i warunkowym. Dodatkowo można wyznaczyć obszar zarządzania ryzykiem sytuacji kryzysowych, który jest związany z ryzykiem warunkowym. Przeprowadzona dyskusja podejść w świetle nauk o bezpieczeństwie oraz nauk o zarządzaniu wskazuje, że w ujęciu funkcjonalnym cele i działania realizowane przez zarządzanie kryzysowe należy lokować w obszarze logistyki społecznej.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rozdział IV
Zarządzanie ryzykiem w administracji publicznej

Rozważania prowadzone w kolejnym rozdziale odnoszą się do tezy nr 3 (w odniesieniu do form zarządzania ryzykiem realizowanych samodzielnie przez administrację publiczną oraz w interakcji z operatorami IK) oraz do tezy nr 4 (w odniesieniu do celów działania organizacji zarządzania kryzysowego, które to cele mogą zostać zakłócone przez czynniki wewnętrzne i zewnętrzne). Badania prowadzone były w trzech etapach. W pierwszym określono formy zarządzania ryzykiem, jakie są stosowane w administracji publicznej. Formy te zostały pogrupowane zgodnie z ich zasadniczymi cechami. W drugim etapie badania miały na celu udzielenie odpowiedzi na pytanie pomocnicze postawione we wstępie do opracowania w brzmieniu: Przy jakich uwarunkowaniach struktury powoływane doraźnie w ramach administracji publicznej można uznać za organizacje? W celu udzielenia odpowiedzi stosowano podejście systemowe. W ostatnim etapie badania służyły określeniu celów strategicznych, jakie ma organizacja zarządzania kryzysowego w kontekście możliwości zarządzania ryzykiem. Dla określenia tych celów wykorzystano podejście procesowe.

4.1. Formy postępowania z ryzykiem w administracji publicznej

Jak już wspomniano we wprowadzeniu, jako początek procesu wdrażania zarządzania ryzykiem w administracji publicznej wskazuje się rok 1995, kiedy to dla Australii i Nowej Zelandii został wydany pierwszy standard zarządzania kryzysowego na poziomie krajowym (AS/NZS 4360). Z czasem podobne standardy zostały przyjęte w Kanadzie, Japonii i W. Brytanii (*Enterprise Risk Management – Integrated Framework*). I właśnie w Brytanii taki model zarządzania zaczęto stosować w bardzo szerokim zakresie. Z czasem okazało się, że działania kolejnych agend rządowych oparte na odmiennych standardach wymuszają konieczność ujednolicenia stosowanego podejścia. W efekcie w 2002 r. zaadaptowano dla potrzeb administracji publicznej zintegrowane zarządzanie kryzysowe (*Enterprise Risk Management*) (*Risk: Improving government's capability to handle risk and uncertainty*). Po jego wprowadzeniu, w zależności od skali zaangażowania państwa i stopnia uciążliwości wprowadzonych regulacji, wyróżnia się dziewięć reżimów zarządzania ryzykiem (Hood, Rothstein, Baldwin 2004).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

W Polsce podjęto próbę wdrożenia zarządzania ryzykiem na wzór brytyjski. Ministerstwo Finansów zamówiło i opublikowało w 2007 r. podręcznik *Zarządzanie ryzykiem w sektorze publicznym – podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce*, jednak ostatecznie podejścia zintegrowanego nie wdrożono. Efektem prac ministerstwa finansów jest natomiast wdrożenie zarządzania ryzykiem w sektorze finansów publicznych (Frańczuk 2011) oraz stopniowe wdrażanie podejścia projektowego do realizacji inwestycji (*Strategia na rzecz Odpowiedzialnego Rozwoju*). Jednym z elementów podejścia projektowego jest zarządzanie ryzykiem (Wodecka-Hyjek 2010).

Oba przypadki dotyczą postępowania z ryzykiem w przypadku gdy przyczyna i skutek leżą wewnątrz organizacji, jaką jest administracja publiczna. Jednak do zarządzania ryzykiem odwołują się regulacje prawne dotyczące wielu innych obszarów i podmiotów, w tym również podmiotów spoza administracji publicznej. W zależności od skali ingerencji obowiązujących regulacji możemy wyróżnić kilka zasadniczych reżimów prawnych.

1. Państwo jako właściciel ryzyka. Dla niektórych rodzajów zagrożeń, ze względu na ich publiczny charakter (Ciekanowski 2010), państwo reguluje wszystkie obszary związane z monitorowaniem i zwalczaniem zagrożenia. Jest to związane z zasadniczymi funkcjami państwa, które „w pierwszym rzędzie powołane jest do tego, aby chronić swoich członków przed niebezpieczeństwami, a w razie ich powstania, zwalczać i usuwać szkody stąd powstałe" (Kasznica 1946). Realizując powyższy cel, państwo zapewnienia porządek i bezpieczeństwo publiczne oraz ochronę mienia i zdrowia obywateli (Oniszczuk 2008). Jest to realizowane poprzez budowanie systemów wykrywania zagrożenia, tworzenie i utrzymywanie służb reagowania oraz tworzenie prawa, w tym prawa powszechnie obowiązującego. Wśród zagrożeń, z którymi państwo musi się zmierzyć, są zagrożenia naturalne, na których istnienie człowiek nie ma wpływu (Bonisławska 2012). Zagrożeniem, dla którego poziom ryzyka jest uważany za najwyższy (KPZK 2013/2015, s. 7), jest powódź. Sposób postępowania z tym zagrożeniem reguluje ustawa Prawo wodne (DzU z 2017 r. poz. 1121) będąca implementacją dyrektywy Parlamentu Europejskiego i Rady w sprawie oceny ryzyka powodziowego i zarządzania nim (DzUrz UE L 288/27, rozdz. III). W pierwszym etapie prezes Krajowego Zarządu Gospodarki Wodnej przygotowuje wstępną ocenę ryzyka powodziowego, na tej podstawie mapy zagrożenia powodziowego i ostatecznie mapy ryzyka powodziowego (DzUrz UE L 288/27, art. 90 ust. 1). Na bazie map prezes KZGW w uzgodnieniu z ministrem właściwym do spraw gospodarki wodnej opracowuje plany zarządzania ryzykiem powodziowym (DzUrz UE L 288/27, art. 88h). Równolegle mapy stanowią podstawę do opracowania, odpowiednio przez wojewodę, starostę i wójta, planu operacyjnego ochrony przed powodzią[16]. Jak wykazują liczne

[16] Obowiązek opracowania takiego planu znajduje się odpowiednio w ustawie o samorządzie gminnym, samorządzie powiatowym oraz w ustawie o wojewodzie i administracji rządowej w województwie.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

kontrole NIK, tak zbudowana struktura organizacyjna nie zarządza ryzykiem powodziowym we właściwy sposób. Rozproszenie odpowiedzialności pomiędzy różne podmioty (administracja rządowa i samorządowa), wobec braku organu koordynującego powoduje, że plany gminne i powiatowe nie są skorelowane z planem wojewódzkim. Z kolei brak obowiązujących standardów sprawia, że zawartość magazynów przeciwpowodziowych jest przypadkowa i nie wynika z oceny ryzyka. W efekcie system zarządzania ryzykiem powodziowym uważany jest za mało efektywny.

2. Państwo jako regulator. Oddziaływania administracji publicznej na podmioty zewnętrzne polega na wzmocnieniu systemu samoregulacji (Power 2004). Podejście samoregulacyjne polega na obowiązku ujawniania wyników kontroli wewnętrznej. Regulacje prawne sprowadzają się do obowiązku przeprowadzania audytu i przekazywania właściwym władzom jego wyników lub do publikowania wyników audytu przeprowadzonego przez niezależny podmiot zewnętrzny. Takie podejście jest charakterystyczne dla regulacji obszaru bankowego (DzU z 2017 r. poz. 637) i firm giełdowych (Nartowski 2016).
3. Państwo jako *Risk Manager*. Przy tym podejściu państwo ściśle reguluje zasady zarządzania ryzykiem, pozostawiając odpowiedzialność za ich przestrzeganie w rękach podmiotu, którego regulacja dotyczy. Elementem sprawdzającym jest audyt zewnętrzny lub kontrola prowadzona przez uprawnione jednostki sektora administracyjnego (np. NIK). Przykładem takiego rozwiązania mogą być regulacje dotyczące funkcjonowania giełdy (DzU z 2016 r. poz. 1636, art. 110b).
4. Państwo jako instytucja certyfikująca. Administracja państwowa określa ściśle sposób prowadzenia oceny ryzyka, zasady postępowania z ryzykiem, narzuca obowiązek certyfikacji personelu, wyrobów i ewentualnie procesów oraz dokonuje kontroli przestrzegania przez podmiot zgodności zarówno z przepisami, jak i stosowanymi procedurami. Takie podejście jest stosowane np. w obszarze bezpieczeństwa żywnościowego (DzU z 2017 r. poz. 1226) produkcji leków, ocenie ryzyka zawodowego (DzU z 2003 r. nr 169, poz. 1650 ze zm., § 37–39).
5. Państwo jako jednostka standaryzacyjna. Jest to jedna z najostrzejszych form ingerencji administracji publicznej stosowana np. w odniesieniu do ochrony informacji niejawnych. W tym przypadku narzucono zasady oceny ryzyka i postępowania z ryzykiem (DzU z 2016 r. poz. 1167 ze zm., art. 2, 15, 49), łącznie z obowiązkiem okresowego przeprowadzania ponownej oceny ryzyka. Wprowadzono obowiązek audytu wstępnego, przed uzyskaniem certyfikatu, obowiązek certyfikacji (obejmujący m.in. osoby, proces postępowania z informacją niejawną, urządzenia służące do wytwarzania i przesyłania informacji i warunki techniczne). Wprowadzono minimalne

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

standardy bezpieczeństwa, które jednostka posługująca się materiałami niejawnymi powinna podwyższyć adekwatnie do przeprowadzonej oceny ryzyka (DzU z 2011 r. nr 159, poz. 948, rozdział 3). Określono minimalną wymaganą strukturę organizacyjną komórek zajmujących się informacją niejawną, łącznie z wymaganiami dotyczącymi szkoleń osób w nich pracujących. Funkcję jednostki audytującej, certyfikującej i kontrolującej powierzono Agencji Bezpieczeństwa Wewnętrznego oraz Służbie Kontrwywiadu Wojskowego, przy czym ABW jest z mocy ustawy krajową władzą bezpieczeństwa (DzU z 2016 r. poz. 1167 ze zm., art. 10 i 11).

Analizując powyższe przypadki, należy zwrócić uwagę na dwa elementy. W każdym z nich nie przewiduje się działań operacyjnych (ratowniczych), a administracja publiczna, nakładając obowiązki na poszczególne podmioty, kładzie nacisk na działania w fazie zapobiegania zagrożeniu. Jest to więc działanie nakierowane na zmniejszanie podatności. Ponadto wszystkie te regulacje pozostawiają odpowiedzialność za zmaterializowanie się ryzyka w rękach podmiotu zarządzającego ryzykiem. Formalnie administracja żadnej odpowiedzialności na siebie nie bierze. W rzeczywistości jednak zastosowanie nawet miękkich form oddziaływania na podmioty gospodarcze poprzez określenie sposobu zarządzania ryzykiem już może sprawić, że administracja stanie się współodpowiedzialną za zmaterializowanie się ryzyka. Przykładowo, kiedy w 1998 r. pod zarzutem seryjnego mordowania pacjentów został aresztowany Harold Frederic Shipman, lekarz domowy z Manczesteru, zarzuty o brak właściwego nadzoru nad bezpieczeństwem pacjentów były kierowane wobec agencji (*General Medical Council*) nadzorującej funkcjonowanie pomiotów leczniczych w Wielkiej Brytanii (Power 2004). Zarzuty dotyczyły zarówno braku nadzoru nad wdrażaniem procedur zarządzania ryzykiem, jak i stwarzania sytuacji, w której przestrzeganie reguł jest ważniejsze niż dobro pacjenta. Innym efektem ubocznym narzucania podmiotom gospodarczym zasad postępowania z ryzykiem może być outsourcing procesów podlegających zbyt dolegliwym regulacjom. Przykładem takiej sytuacji może być powstanie usług zwanych zbiorczo logistyką wartości pieniężnych. Chcąc uniknąć rygorów związanych z transportem i przechowywaniem wartości pieniężnych (DzU z 2016 r., poz. 793), banki stopniowo wycofują obrót gotówkowy ze swojej działalności, powierzając to zadanie specjalistycznym firmom zewnętrznym. Firmy te na zlecenie banku odbierają utarg od jednostek handlowych, przewożą do własnych centrów obsługi gotówki, dokonują zmian na koncie zlecającego usługę, a na koniec zasilają bankomaty. W efekcie bank nie ma praktycznie kontaktu z gotówką, poza utrzymywaniem pogotowia kasowego na możliwie najniższym poziomie. To posunięcie, zapewne uzasadnione biznesowo, z punktu widzenia zarządzania kryzysowego spowodowało powstanie nowego ryzyka. W przypadku awarii bankomatów lub systemu transakcyjnego powstaje sytuacja, gdy klient banku traci dostęp do gotówki. Nie może jej otrzymać ani z banku, który nie posiada technicznych możliwości przechowywania większych kwot, ani z firmy zajmującej się obsługą

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

gotówki, gdyż ta nie posiada punktów obsługi klienta indywidualnego. Tę sytuację można określić jako przypadek wyłonienia się nowego rodzaju usługi o nazwie „dostęp do środków płatniczych"[17]. Zdefiniowaniem tej usługi i jej utrzymaniem w sytuacjach nadzwyczajnych będzie musiała zająć się administracja publiczna. W sumie narzucenie podmiotom gospodarczym ostrych rygorów postępowania z ryzykiem utraty środków pieniężnych wygenerowało nowy rodzaj ryzyka, którego właścicielem stała się administracja publiczna.

4.2. System zarządzania kryzysowego jako element organizacji państwa

Jak już omówiono w II rozdziale, realizowanie zadań zarządzania kryzysowego zostało oparte na strukturach administracji publicznej, począwszy od poziomu centralnego (Rada Ministrów i poszczególni ministrowie) poprzez szczebel regionalny (wojewodowie) po szczebel samorządowy (starostowie i wójtowie). Stosowanie wobec tak zdefiniowanej struktury pojęcia „organizacja" wymaga szczegółowej analizy, ze względu na niejednoznaczne zależności występujące pomiędzy poszczególnymi jej uczestnikami. Ta niejednoznaczność relacji wynika z faktu, że administracja samorządowa nie podlega organizacyjnie administracji rządowej. Podlega jedynie nadzorowi z punktu widzenia legalności (Konstytucja RP, art. 172 ust. 1). Wyklucza to w konsekwencji możliwość ingerencji nadzorczych w kontekście efektywności czy celowości. Ponadto wymienione organy nie są formalnie podporządkowane jednemu decydentowi. W takich przypadkach, zarówno wobec administracji publicznej, jak i wobec wielopodmiotowych struktur tworzonych na bazie administracji, nie stosuje się pojęcia „organizacja", lecz „system" (Krajowy System Ratowniczo-Gaśniczy, system ochrony zdrowia, system zarządzania kryzysowego itp.).

Traktowanie administracji jako systemu było przedmiotem badań z pozytywnym efektem (Wrzosek 2008). Pozostaje stwierdzić, czy podejście systemowe może być stosowane wobec struktur wielopodmiotowych tworzonych przez administrację w sposób trwały lub doraźny. W pierwszym kroku zatem należy zdefiniować pojęcie „system":

„System jest to wyodrębniony zbiór elementów (materialnych lub abstrakcyjnych), wzajemnie powiązanych, rozważany jako całość z określonego punktu widzenia, mający przy tym takie właściwości, których nie posiadają jego elementy" (Jajuga i in. 1993). Lub nieco inaczej (Krzyżanowski 1999) – „Przez system SYS rozumie się zbiór elementów e, wyróżnionych w jakimkolwiek przedmiocie P ze względu na zachodzące między nimi stosunki S_{up}, wyrażające jakieś uporządkowanie:

$$SYS = [\{e(P)\}, S_{up}]".$$

[17] Analiza zagrożeń związanych z funkcjonowaniem centrów obsługi gotówki, RCB 2016 – materiał niejawny.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Z tą definicją koreluje następujące spostrzeżenie: „System musi posiadać pewną cechę (cechę systemową), czyli własność, która charakteryzuje system jako całość, lecz której nie mają jego poszczególne elementy" (Sienkiewicz 1994).

Przechodząc na grunt nauk o zarządzaniu, należy zwrócić uwagę na następującą definicję: „Organizacja jest szczególnym przypadkiem systemu, scharakteryzowanym przez specyficzne okoliczności, ze względu na które rozpatrujemy jego strukturę" (Zieleniewski 1975). Do tej definicji nawiązuje następujące stwierdzenie: „Organizacja jest to system, którego uporządkowanie polega przede wszystkim na tym, że funkcjonalnie zróżnicowane jego części w zasadzie współprzyczyniają się do powodzenia całości, a powodzenie całości jest istotnym warunkiem powodzenia części" (Krzyżanowski 1999).

Z przeprowadzonej analizy wynika, że systemy organizacyjne tworzone na stałe lub doraźnie w ramach administracji można traktować jako rodzaj organizacji, o ile posiadają cechy systemowe stanowiące o celu ich istnienia. Poszukując tych cech, należy zauważyć, że w przeciwieństwie do ustaw regulujących specjalistyczne obszary działalności administracji, służb inspekcji i straży (ochrona przeciwpożarowa, zwalczanie epidemii itp.), zarządzanie kryzysowe nie tworzy w sposób całościowy nowego obszaru zadaniowego. Zamiast tego, bazując na istniejących rozwiązaniach prawnych, strukturach organizacyjnych i zasobach, uzupełnia je o elementy planowania i koordynacji. Dzięki temu można osiągnąć efekt synergii, bez dublowania kosztów (Skomra 2016). Zatem zasadniczą funkcją badanego systemu jest koordynacja wysiłków różnych podmiotów na rzecz realizacji wspólnego celu. Pod pojęciem „koordynacja" należy przy tym rozumieć „włączanie do działania wszystkich i tylko tych elementów (ludzi wykonujących określone czynności i innych zasobów spełniających określone funkcje), które są niezbędne do zapewnienia powodzenia, i to włączenia ich tak, aby elementy te maksymalnie przyczyniały się do powodzenia całości (instytucji, zespołów lub ich fragmentów) – a więc włączanie ich we właściwej jakości i ilości i we właściwej chwili" (Zieleniewski 1975). Koordynacja poszczególnych elementów powinna być realizowana pod względem jakościowym, ilościowym i czasowym. To podejście nawiązuje do prawa harmonii sformułowanej na początku XX wieku przez K. Adamieckiego (Adamiecki 1938).

Praktycznym wymiarem funkcji koordynacyjnej jest m.in. powoływanie w sytuacjach kryzysowych struktur doraźnych (zespoły zarządzania kryzysowego), które mają w swoim założeniu pokonać ograniczenia formalne i techniczne jakie obowiązują poszczególnych jej uczestników (Skomra 2005). Zdolność do pokonania tych ograniczeń jest cechą pozwalającą uznać, że struktura organizacyjna zarządzania kryzysowego jest systemem.

4.3. Ujęcie procesowe w zarządzaniu ryzykiem

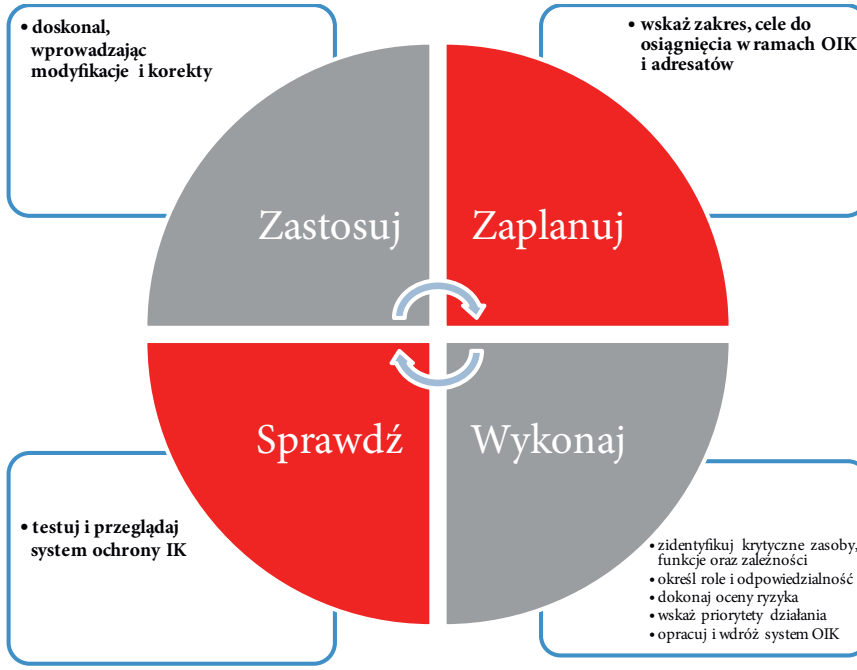
Włączenie do obszaru zarządzania kryzysowego zagadnień związanych z infrastrukturą krytyczną spowodowało, że zadania realizowane na rzecz jej ochrony

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

zaczęły być postrzegane w ujęciu procesowym równolegle do podejścia systemowego charakteryzującego formalną strukturę wynikającą z UZK. Wprowadzenie podejścia procesowego jest ściśle związane z obowiązkiem zarządzania ciągłością działania (DzU z 2010 r. nr 83, poz. 542, § 2 ust. 3 pkt. 4) opartą m.in. na normach (NPOIK, załącznik nr 1, s. 42):

- PN-EN ISO 9001. Systemy zarządzania jakością,
- PN-ISO 31000. Zarządzanie ryzykiem,
- PN-EN ISO 22301. Bezpieczeństwo powszechne. Systemy zarządzania ciągłością działania.

Pierwszym warunkiem wdrożenia ciągłości działania jest zidentyfikowanie procesów głównych, pomocniczych oraz związanych z procesami zarządzania. Wszystkie działania związane z bezpieczeństwem obiektów powinny być realizowane w cyklu Deminga definiującego zasady ciągłego doskonalenia.


• doskonal, wprowadzając modyfikacje i korekty
• wskaż zakres, cele do osiągnięcia w ramach OIK i adresatów
Zastosuj
Zaplanuj
Sprawdź
Wykonaj
• testuj i przeglądaj system ochrony IK
• zidentyfikuj krytyczne zasoby, funkcje oraz zależności
• określ role i odpowiedzialność
• dokonaj oceny ryzyka
• wskaż priorytety działania
• opracuj i wdróż system OIK

Rys. 3. Cykl Deminga

Źródło: NPOIK, s. 28

Początkowo obowiązek wdrożenia ciągłości działania dotyczył operatorów IK (część z nich jest podmiotami administracji publicznej), ale z czasem został rozszerzony na urzędy obsługujące ministrów – gospodarzy poszczególnych systemów IK (NPOIK, s. 21). Niezależnie od obowiązków i dobrych praktyk w związku z ochroną IK część urzędów administracji publicznej wdraża elementy podejścia procesowego w celu poprawy jakości usług lub ze względów wizerunkowych

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

(Szumowski 2009). Przyjmując założenie, że każdą czynność lub zbiór czynności można przedstawić jako proces, w którym z nakładu otrzymujemy rezultaty, w jednostkach administracji publicznej za proces można uznać ciąg działań służący wydaniu decyzji, oferowaniu usługi lub informacji albo szerzej – jako łańcuch sekwencyjnych czynności, które zmieniają mierzalne elementy na wejściu (dokumenty, informacje, metody, decyzje) w mierzalne elementy wyjścia (informacje, decyzje, usługi publiczne) (Krukowski 2011). Porównanie podejścia procesowego i funkcjonalnego przedstawiono w tabeli nr 19.

Tabela 19. Cechy podejścia procesowego i funkcjonalnego w organizacji publicznej

Cechy	*Podejście procesowe*	*Podejście funkcjonalne*
Kluczowy obszar	Jakość usług	Procedury świadczonych usług
Koordynacja pracowników	Wysoka; praca zespołowa	Niska; koordynacja między zespołami
Zarządzanie	Procesowe	Funkcjonalne
Orientacja strategiczna	Na klienta	Na procedury

Źródło: Krukowski, 2011, s. 24

Podstawy teoretyczne pozwalające przejść na podejście procesowe w administracji publicznej istnieją pod nazwą „Nowe zarządzanie w sektorze publicznym" (Krynicka 2006). Jednak dopiero cyfryzacja administracji oparta na realizowanych procesach przyśpieszyła te zmiany. Przykładowo zorientowanie na procesy w administracji publicznej i usługi, jakie ona zapewnia, jest jedną z czterech podstawowych zasad, na których opiera się informatyzacja zintegrowana wdrażana w ramach e-administracji (Boni 2012). W efekcie w administracji publicznej można obserwować ten sam trend, który nastąpił w działalności biznesowej, gdzie podejście procesowe zaczyna dominować nad podejściem systemowym (Zawiła-Niedźwiecki, Gołąb 2010). Ten kierunek działań zapewne będzie się pogłębiać w związku z postanowieniami dyrektywy NIS. Dyrektywa nakłada obowiązek wyłonienia przez państwa członkowskie tzw. „usług kluczowych", tj. takich, które służą utrzymaniu „krytycznej działalności społecznej i gospodarczej". Wykaz sektorów, w których należy wyłonić usługi kluczowe, przedstawiono w tabeli nr 20.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 20. Wykaz sektorów objętych wymogami dyrektywy NIS

Sektor	*Podsektor*	*Rodzaj podmiotu*
Energetyka	Energia elektryczna	przedsiębiorstwa energetyczne
		operatorzy systemu dystrybucyjnego
		operatorzy systemu przesyłowego
	Ropa naftowa	operatorzy ropociągów
		operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej
	Gaz	przedsiębiorstwa dostarczające gaz
		operatorzy systemu dystrybucyjnego
		operatorzy systemu przesyłowego
		operatorzy systemu magazynowania
		operatorzy systemu LNG
		przedsiębiorstwa gazowe
		operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego
Transport	Transport lotniczy	przewoźnicy lotniczy
		zarządzający portem lotniczym, porty lotnicze oraz jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych
		operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC)
	Transport kolejowy	zarządcy infrastruktury
		przedsiębiorstwa kolejowe
	Transport wodny	armatorzy śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów
		organy zarządzające portami

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Sektor	*Podsektor*	*Rodzaj podmiotu*
		operatorzy systemów ruchu statków
	Transport drogowy	organy administracji drogowej
		operatorzy inteligentnych systemów transportowych
Bankowość, instytucje kredytowe		
Infrastruktura rynków finansowych		operatorzy systemu obrotu
Służba zdrowia	Ośrodki opieki zdrowotnej (w tym szpitale i prywatne kliniki)	
Zaopatrzenie w wodę pitną i jej dystrybucja		dostawcy i dystrybutorzy „wody przeznaczonej do spożycia przez ludzi”
Infrastruktura cyfrowa		IXP
		dostawcy usług DNS
		rejestry nazw TLD

Źródło: DzUrz UE L 194/1, zał II

Formalnie dyrektywa odnosi się wyłącznie do bezpieczeństwa sieci i systemów teleinformatycznych w ww. sektorach. Jednak w celu szerszego zastosowania podejścia jakościowego w dziedzinie ochrony IK w Rządowym Centrum Bezpieczeństwa trwają prace koncepcyjne nad nową procedurą wyłaniania IK na podstawie wcześniej zdefiniowanej listy usług kluczowych. Aby zrozumieć ideę podejścia usługowego, należy zauważyć, że operator IK nie jest właścicielem wszystkich rodzajów ryzyka (a więc i skutków zdarzeń niekorzystnych) związanych z prowadzoną działalnością. W skali makroekonomicznej działania podmiotów gospodarczych mają wymiar społeczny i w tym przypadku właścicielem ryzyka staje się państwo. Przykładowo brak prądu w skali mikroekonomicznej oznacza dla elektrowni brak zysków i ewentualnie konieczność wypłaty odszkodowań. W skali makroekonomicznej brak prądu może oznaczać dla odbiorcy brak dostępu do pieniądza (nie działają bankomaty), brak możliwości przemieszczania się (niemożność zatankowania pojazdu) czy trudności z zakupem żywności (znaczna część produktów spożywczych wymaga chłodni). Te rodzaje ryzyka nie wchodzą w zakres odpowiedzialności elektrowni. Narzędziem do regulacji odpowiedzialności i podejmowania działań są w takiej sytuacji rozwiązania ustawowe. Różnice w zarządzaniu ryzykiem w obu skalach przedstawiono w tabeli nr 21.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 21. Różnice w zarządzaniu ryzykiem w skali makro- i mikroekonomicznej

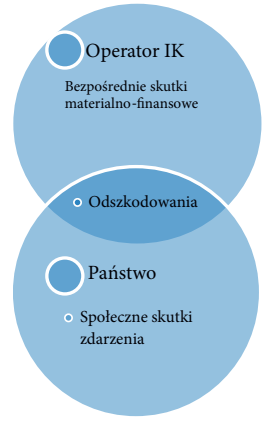
Skala zarządzania	makroekonomiczna	mikroekonomiczna
Wymiar zarządzania	społeczny	biznesowy
Uregulowania	ustawowe	normatywne

Źródło: Zapłata, Kaźmierczak 2011, s. 35

Właścicielem ryzyka bezwarunkowego może być sama administracja, i w tym przypadku zmaterializowanie się ryzyka może oddziaływać zarówno na ludzi, jak i na podmioty gospodarcze. Przykładowo dane, jakie podmioty gospodarcze uzyskują z systemu rejestrów państwowych, są zasobem wejściowym w procesach realizowanych przez te podmioty. W innych przypadkach administracja dostarcza narzędzi do realizacji niektórych procesów biznesowych (np. aplikacje do rozliczania podatków) i w efekcie staje się źródłem ryzyka operacyjnego dla podmiotów uzależnionych od tych narzędzi lub dostarczanych danych.

4.4. Cele systemu zarządzania kryzysowego

Zasadniczym celem funkcjonowania zarządzania kryzysowego jest łagodzenie potencjalnych lub rzeczywistych skutków społecznych zmaterializowania się ryzyka. Zakres tych skutków można wywnioskować z definicji zawartych w UZK. Jak już wyjaśniono w rozdziale I ilekroć mowa o sytuacji kryzysowej należy przez to rozumieć „sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej". W odniesieniu do obiektów IK ustawa posługuje się dodatkowo takimi pojęciami jak „kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców" (UZK, art. 3). W ujęciu całościowym zarządzanie skutkami zdarzeń z punktu widzenia właściciela ryzyka przedstawiono na schemacie nr 10.



Schemat 10. Podział skutków zdarzenia ze względu na podmiot odpowiedzialny
Źródło: opracowanie własne

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

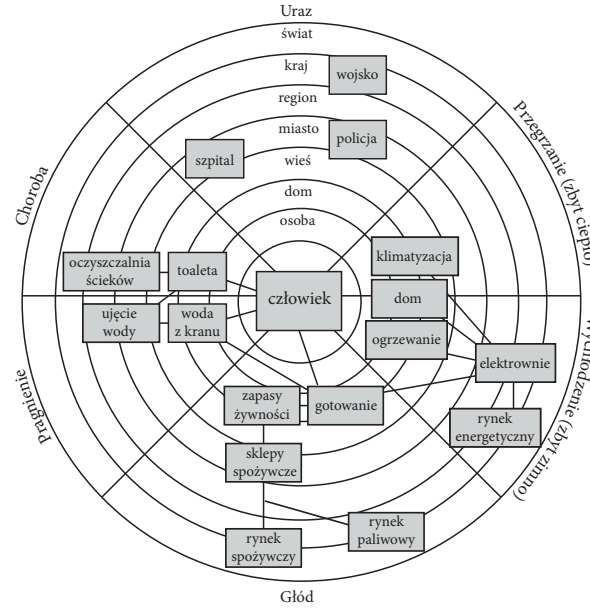
Powyższa zależność istnieje obiektywnie niezależnie od metody wyłaniania IK, jednak łatwiej ją dostrzec, jeśli na problem usług krytycznych spojrzy się z punktu widzenia odbiorcy. Uogólniając powyższe spostrzeżenie, omawiany schemat można zinterpretować następująco. Dla właściciela (operatora IK) infrastruktura przez niego zarządzana powinna służyć przede wszystkim osiąganiu celów biznesowych (zysku). Jednocześnie ta sama infrastruktura powinna, poza celami biznesowymi, uwzględniać aspekt społeczny, o ile prowadzona działalność lub jej czasowe zaprzestanie może wywołać skutki dla ludzi, ich mienia lub środowiska. Niezależnie jednak od prób zdefiniowania, czym jest IK jednocześnie z biznesowego i społecznego punktu widzenia, należy stwierdzić, że usługi (oraz związane z nimi procesy, podprocesy i procedury) świadczone przez tę infrastrukturę można podzielić na takie, które służą wyłącznie celom biznesowym, i takie, których dysfunkcja wywoła społeczne skutki na tyle dolegliwe, że zarządzać nimi będzie musiało państwo. Omawianą zależność można też przedstawić w aspekcie zarządzającego ryzykiem. Przykładowo dla firmy zapewniającej dostawy wody ryzykiem bezwarunkowym jest związana z potencjalną awarią możliwość utraty dochodów i konieczność wypłaty odszkodowań za niezrealizowane umowy. Ryzykiem warunkowym jest natomiast konieczność ewakuacji szpitala pozbawionego dostaw wody. Właścicielem tego drugiego ryzyka jest jednak nie dostawca wody, lecz administracja publiczna.

Aby wyodrębnić usługi o krytycznym znaczeniu dla mieszkańców, można posłużyć się metodyką „6 ways to die". Zgodnie z tym podejściem rolą administracji publicznej jest eliminacja sześciu czynników, które mogą spowodować śmierć człowieka. Tymi czynnikami są:

- głód,
- pragnienie,
- zranienia,
- choroby,
- zbyt wysoka temperatura,
- zbyt niska temperatura.

Schemat nr 11 przedstawia powiązania ww. czynników z usługami jakie są z nimi skojarzone oraz poziomami administracji odpowiedzialnymi za zapewnienie tych usług.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353



Schemat 11. Mapa infrastruktury krytycznej i jej poziomów.
Źródło: Bennett, Gupta 2010; za: Pyznar, Abgarowicz 2014, s. 16

Jak widać na schemacie, każdemu czynnikowi mogącemu spowodować śmierć osoby można przypisać procesy i systemy oraz szczebel administracji odpowiedzialny za ich sprawne działanie (co nie oznacza, że administracja musi być operatorem danego systemu). Przykładowo w ramach systemu zaopatrzenie w wodę można wyodrębnić procesy:

- ujmowanie i uzdatnianie wody przeznaczonej do spożycia przez ludzi,
- dostarczanie wody przeznaczonej do spożycia przez ludzi,
- odbiór i oczyszczanie ścieków.

Każdemu z nich można przypisać prawdopodobieństwo awarii i ocenić spodziewane skutki, wyliczając poziom ryzyka. Skutki można sparametryzować i przypisać do poszczególnych poziomów administracji, uzyskując w ten sposób podział na krytyczną infrastrukturę lokalną, regionalną i centralną (krajową). Przykładowo lokalna IK może oznaczać brak usługi dla 100 tys. osób i więcej, regionalna powyżej 300 tys., zaś krajowa powyżej 500 tys. Przy okazji każdemu poziomowi można przypisać odpowiedni poziom ochrony tak by niezbędne nakłady finansowe były adekwatne do poziomu ryzyka.

Proces wyłaniania obiektów IK przy takim podejściu składałby się z dwóch etapów:

- zidentyfikowanie usług krytycznych świadczonych przez dany obiekt;
- określenie skutków dysfunkcji danej usługi i porównanie z kryteriami przekrojowymi definiującymi IK lokalne, regionalne i krajowe.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Na koniec można wskazać niezbędny poziom zabezpieczeń adekwatny do klasy IK (lokalna, regionalna lub krajowa) i poziomu ryzyka. Przedstawiony sposób wyłaniania IK oparty o funkcje i procesy rozszerza podejście stosowane w omówionej już dyrektywie NIS. Jednocześnie należy zauważyć wieloaspektowy wymiar stosowania metodyki „6 ways to die". Metodyka nie tylko pozwala wyłaniać procesy kluczowe, ale wskazuje zasadnicze cele budowania systemów ratowniczych, zarządzania kryzysowego, a wręcz podstawowy cel istnienia państwa. Jednocześnie można dostrzec, że zagadnienia, wobec których metodyka ma zastosowanie, mieszczą się w obszarze logistyki społecznej. Jak już wcześniej zostało wspomniane, priorytetem tej logistyki jest jakość życia społeczeństwa.

4.5. Podsumowanie rozdziału

Dotychczasowe formy zarządzania ryzykiem stosowane w administracji publicznej opierają się na stanowieniu i egzekwowaniu prawa. Działania te nie przewidują i nie odnoszą się do reakcji na zmaterializowanie się ryzyka.

Wymagane postanowieniami UMOL zarządzanie ryzykiem wymaga zupełnie innych metod postępowania, co oznacza konieczność stworzenia nowych ram prawnych i organizacyjnych.

Strukturom, których zadaniem jest zarządzanie tym ryzykiem (nawet jeśli tworzone są doraźnie), można przypisać miano organizacji. Tak określonej organizacji można wyznaczyć cele jej funkcjonowania oraz wyznaczyć procesy, które służą realizacji tych celów.

Z punktu widzenia logistyki społecznej występuje współzależność pomiędzy administracją publiczną a operatorami IK. Państwo określa ramy prawne działania takich podmiotów (np. poprzez wymagania dotyczące planów ochrony IK), czerpie korzyści z ich funkcjonowania (np. podatki), ale jednocześnie ponosi odpowiedzialność za społeczne skutki braku dostępu do usług świadczonych przez operatorów IK. Te współzależności nie zostały jak dotąd opisane ani w przepisach prawa, ani w literaturze przedmiotu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rozdział V
Elementy zarządzania ryzykiem w publicznym zarządzaniu kryzysowym

Kolejna część procesu badawczego odnosi się do pytania będącego głównym problemem badawczym: Jakie zależności występują pomiędzy ryzykiem operacyjnym a pozostałymi rodzajami ryzyka, którymi zarządza się w ramach publicznego zarządzania kryzysowego? Badania w niniejszym rozdziale mają charakter teoriotwórczy i oparte są o indukcję. W celu ujawnienia zależności, jakie łączą ryzyko operacyjne ze wszystkimi aspektami zarządzania kryzysowego zastosowano metodę analizy źródeł oraz metodę *case study*. Badania wiążą się z tezą nr 5 (w zakresie możliwości zarządzania ryzykiem operacyjnym w różnych aspektach działań).

5.1. Ryzyko operacyjne w zarządzaniu kryzysowym

Na podstawie przeprowadzonych rozwiązań można stwierdzić, że zarządzanie kryzysowe jest formą organizacji. W ujęciu systemowym składa się z elementów o zróżnicowanej strukturze. Są nimi organy zarządzania kryzysowego, stałe i powoływane doraźnie komórki obsługujące te organy, a nawet podsystemy (ochrony zdrowia, ochrony ludności itp.). System ma charakter otwarty, co oznacza, że występuje sprzężenie zwrotne pomiędzy systemem a jego otoczeniem. Z jednej strony reakcje systemu są uzależnione od warunków zewnętrznych, a z drugiej strony reakcje systemu mają wpływ na otoczenie (Stoner, Freeman, Gilbert 2001).

Wszystkie elementy systemu powiązane są ze sobą poprzez zależności (wsparcie, koordynacja lub zwierzchnictwo). Wewnątrz systemu istnieje przepływ informacji (monitoring zagrożeń i prowadzonych działań, przekazywanie decyzji i raportów, itp.) oraz zasobów (udzielanie wsparcia technicznego i finansowego). System ma cel główny, którym jest łagodzenie potencjalnych lub rzeczywistych skutków społecznych zmaterializowania się ryzyka bez względu na jego źródło. Te skutki społeczne zostały ustawowo określone jako negatywne oddziaływanie na ludzi, mienie w znacznych rozmiarach lub środowisko. Tak zdefiniowane skutki są jednocześnie granicami systemu w ujęciu podmiotowym. System zasadniczo opiera się na administracji publicznej i jej hierarchicznej strukturze, ale ma własny ustawowo zdefiniowany zakres zadań, odmienny obieg informacji, własny cykl planowania i odrębne dokumenty planistyczne. Ponadto swoim zasięgiem obejmuje podmioty spoza administracji publicznej (operatorów IK).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

System, jak każda inna organizacja, jest narażony na ryzyko operacyjne. Ryzyko operacyjne jest pojęciem wprowadzonym na potrzeby działań sektora bankowego przez komitet bazylejski (*Basel Committe on Banking Supervision*). Polską implementacją zaleceń opracowanych przez komitet jest „Rekomendacja M" dotycząca zarządzania ryzykiem operacyjnym w bankach (DzUrz KNF z 2013 r. poz. 6). Wykaz rodzajów zdarzeń operacyjnych wynikających z rekomendacji M zawiera tabela nr 22.

Tabela 22. Klasyfikacja rodzajów zdarzeń operacyjnych zgodnie z dyrektywą M

Rodzaj zdarzenia	*Definicja*	*Kategoria zdarzenia w ramach rodzaju*	*Przykłady zdarzeń operacyjnych*
1	2	3	4
1. Oszustwa wewnętrzne	Straty spowodowane celowym działaniem polegającym na defraudacji, sprzeniewierzeniu majątku, obejściach regulacji, przepisów prawa lub przepisów wewnętrznych przedsiębiorstwa, wyłączając straty wynikające z różnicowania/dyskryminacji pracowników, które dotyczą co najmniej jednej strony wewnętrznej.	1) Działania nieuprawnione	1) Działania nierejestrowane (zamierzone) 2) Nieautoryzowane transakcje (poniesiona strata) 3) Błędna wycena transakcji (zamierzona)
		2) Kradzież i oszustwo	1) Oszustwo, oszustwo kredytowe, bezwartościowy depozyt 2) Kradzież, wymuszenie, defraudacja, rabunek 3) Sprzeniewierzenie aktywów 4) Zamierzone zniszczenie aktywów 5) Fałszerstwo 6) Oszustwo czekowe 7) Przemyt 8) Przejęcie rachunku, podszycie itp. 9) Niezgodności podatkowe, unikanie podatków (umyślne) 10) Przekupstwo, łapówkarstwo 11) Wykorzystanie poufnych informacji w transakcji w celu osiągnięcia korzyści (nie na rachunek banku)

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rodzaj zdarzenia	*Definicja*	*Kategoria zdarzenia w ramach rodzaju*	*Przykłady zdarzeń operacyjnych*
1	2	3	4
2. Oszustwa zewnętrzne	Straty spowodowane celowym działaniem polegającym na defraudacji, sprzeniewierzeniu majątku lub obejściu regulacji prawnych przez stronę trzecią.	1) Kradzież i oszustwo	1) Kradzież, rabunek 2) Fałszerstwo 3) Oszustwo czekowe
		2) Bezpieczeństwo systemów	1) Uszkodzenia na skutek działań hakerskich 2) Kradzież informacji (poniesiona strata)
3. Zasady dotyczące zatrudnienia oraz bezpieczeństwo w miejscu pracy	Straty powstałe na skutek działań niezgodnych z przepisami lub porozumieniami dotyczącymi zatrudnienia, bezpieczeństwa i higieny pracy, wypłaty odszkodowań z tytułu uszkodzenia ciała lub straty wynikające z nierównego traktowania i dyskryminacji pracowników.	1) Stosunki pracownicze	1) Zdarzenia związane z wypłatą wynagrodzeń, przekazywaniem innych korzyści oraz z rozwiązywaniem współpracy z pracownikiem 2) Zorganizowane działania związków zawodowych (strajki, protesty)
		2) Bezpieczeństwo środowiska pracy	1) Wypadki na terenie administrowanym przez bank 2) Wypadki przy pracy z powodu nieprzestrzegania przez bank przepisów BHP i ppoż. 3) Inne zdarzenia skutkujące wypłatami odszkodowań dla pracowników
		3) Podziały i dyskryminacja	Wszelkie typy dyskryminacji pracowników
4. Klienci, produkty i praktyki operacyjne	Straty wynikające z niewywiązania się z obowiązków zawodowych względem określonych klientów, będące skutkiem działań nieumyślnych lub zaniedbania (w tym wymagań powierniczych i stosownego zachowania)	1) Obsługa klientów, ujawnianie informacji o klientach, zobowiązania względem klientów	1) Nadużycie zaufania, naruszenie wytycznych w zakresie obsługi klientów 2) Zagadnienia dotyczące należytej staranności w zakresie weryfikacji klienta i dopasowania oferowanych mu produktów (poznaj swego klienta itp.)

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rodzaj zdarzenia	*Definicja*	*Kategoria zdarzenia w ramach rodzaju*	*Przykłady zdarzeń operacyjnych*
1	2	3	4
	lub też związane z charakterem bądź konstrukcją produktu.		3) Ujawnianie informacji dotyczących klientów indywidualnych 4) Naruszenie prywatności 5) Agresywna sprzedaż 6) Agresywny handel na rachunek klienta w celu maksymalizacji prowizji 7) Nieuprawnione użycie informacji poufnej 8) Odpowiedzialność kredytodawcy
		2) Niewłaściwe praktyki biznesowe lub rynkowe	1) Pogwałcenie przepisów antymonopolowych 2) Niewłaściwe praktyki handlowe/rynkowe 3) Manipulacje rynkiem finansowym 4) Wykorzystanie poufnych informacji w transakcji w celu osiągnięcia korzyści (na rachunek banku) 5) Działanie bez licencji 6) Pranie pieniędzy
		3) Wady produktów	1) Wadliwie skonstruowane produkty bankowe (w tym błędy wzorów umów, regulaminów i innych tego typu dokumentów, brak właściwej autoryzacji) 2) Błędy modeli
		4) Klasyfikacja klienta i ekspozycje	1) Dokonywanie oceny profilu klienta niezgodnie z wytycznymi 2) Przekraczanie limitów ekspozycji względem klienta

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rodzaj zdarzenia	*Definicja*	*Kategoria zdarzenia w ramach rodzaju*	*Przykłady zdarzeń operacyjnych*
1	2	3	4
		5) Usługi doradcze	Spory o jakość działalności doradczej świadczonej przez bank
5. Szkody związane z aktywami rzeczowymi	Straty powstałe na skutek straty lub szkody w aktywach rzeczowych w wyniku klęski żywiołowej lub innych wydarzeń.	Klęski żywiołowe i inne zdarzenia	1) Straty powstałe w wyniku klęsk żywiołowych 2) Straty wynikające z działalności terrorystycznej, wandalizmu
6. Zakłócenia działalności banku i awarie systemów	Straty powstałe na skutek zakłóceń działalności banku lub awarii systemów.	Systemy	1) Nieprawidłowe działanie sprzętu 2) Nieprawidłowe działanie oprogramowania 3) Nieprawidłowe działanie sieci telekomunikacyjnych i komputerowych 4) Przerwy w dopływie energii elektrycznej oraz nieprawidłowe działanie urządzeń podtrzymujących zasilanie
7. Wykonanie transakcji, dostawa i zarządzanie procesami operacyjnymi	Straty powstałe na skutek nieprawidłowego rozliczenia transakcji lub wadliwego zarządzania procesami operacyjnymi oraz wynikłe ze stosunków z kontrahentami i sprzedawcami.	1) Wprowadzanie do systemu, wykonywanie, rozliczanie i obsługa transakcji	1) Błędy w komunikacji 2) Błędy wprowadzania, utrzymania i ładowania danych 3) Przeoczenie terminu lub niewywiązanie się z ciążącego obowiązku 4) Błędne działanie modelu lub systemu 5) Błędy księgowe/ błędne przypisanie do rachunku 6) Błędy wykonania innych zadań 7) Niewykonanie dostawy 8) Błędy w zakresie zarządzania zabezpieczeniami transakcji

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rodzaj zdarzenia	*Definicja*	*Kategoria zdarzenia w ramach rodzaju*	*Przykłady zdarzeń operacyjnych*
1	2	3	4
			9) Utrzymywanie danych referencyjnych
		2) Monitorowanie i sprawozdawczość	1) Niewykonanie obowiązku sprawozdawczego 2) Opublikowanie nierzetelnego sprawozdania (poniesiona strata)
		3) Napływ i dokumentacja klientów	1) Zagubienie dokumentacji dotyczącej udzielenia, odwołania pełnomocnictwa oraz klauzul 2) Brak/niekompletność dokumentacji prawnej
		4) Zarządzanie rachunkami klientów	1) Udzielenie dostępu do rachunku osobom nieuprawnionym 2) Błędne dane klienta (poniesiona strata) 3) Wyrządzenie szkody lub straty w aktywach klienta wskutek zaniedbania
		5) Kontrahenci niebędący klientami banku (np. izby rozliczeniowe)	1) Błąd kontrahenta niebędącego klientem banku 2) Spory z kontrahentami niebędącymi klientami banku
		6) Sprzedawcy i dostawcy	1) Wadliwie sporządzone umowy dotyczące powierzania wykonywania czynności bankowych podmiotom zewnętrznym oraz ich niewłaściwe realizowanie 2) Spory ze sprzedawcami i dostawcami

Źródło: Uchwała Nr 8/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach DzUrz KNF z 2013 r. poz. 6

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Pomimo że rekomendacja dotyczy sektora bankowego, ze względu na swój uniwersalny charakter wykaz zdarzeń operacyjnych zawarty w rekomendacji jest adaptowany i stosowany przed inne podmioty gospodarcze i organizacje. Wprawdzie lista zdarzeń operacyjnych zawarta w rekomendacji nie jest logicznie uporządkowana (zawiera jednocześnie ujęcie przyczynowe i skutkowe), to na jej bazie, z punktu widzenia teorii organizacji i zarządzania, można określić podstawowe czynniki ryzyka (Zawiła-Niedźwiecki 2013):

- możliwe są zdarzenia wewnętrzne i zewnętrzne zakłócające działanie organizacji, tzn. naruszające prowadzenie procesów;
- procesy są w określonym stopniu i zakresie podatne na zdarzenia zakłócające;
- określone zasoby są newralgiczne dla utrzymania procesów;
- organizacja może ponosić prawną odpowiedzialność za konsekwencje naruszenia procesów lub zasobów.

Jak widać, przedstawione czynniki ryzyka powiązane są z podejściem procesowym, które to podejście coraz częściej jest stosowane w administracji publicznej, w tym również w zarządzaniu kryzysowym. Przykładowy wykaz procesów realizowanych przez RCB w odniesieniu do zarządzania kryzysowego zawiera tabela nr 23.

Tabela 23. Wykaz podstawowych procesów realizowanych przez Rządowe Centrum Bezpieczeństwa w ramach zarządzania kryzysowego

Nr procesu	*Komórka wiodąca*	*Proces*
	COA	Informowanie o zdarzeniach i zagrożeniach (służba dyżurna)
	COA	Raportowanie okresowe o zagrożeniach (analizy)
	COA	Zapewnienie obiegu informacji w sytuacji kryzysowej (raportowanie sytuacyjne)
	COA	Wymiana informacji w ramach NATO NCRS
	COA	Planowanie i realizacja treningów pk. IMPULS
	COA	Sporządzenie wykazu danych teleadresowych osób/jednostek systemu zarządzania kryzysowego
	COA	Sporządzenie wykazu danych teleadresowych osób/jednostek eksperckich
	Planowanie	Opracowanie Krajowego Planu Zarządzania Kryzysowego
	Planowanie	Opracowanie Raportu o zagrożeniach bezpieczeństwa narodowego
	Planowanie	Opracowanie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego (NCRS)
	Planowanie	Opracowanie Planu Operacyjnego Funkcjonowania RCB
	Planowanie	Organizacja ćwiczeń „Libero”

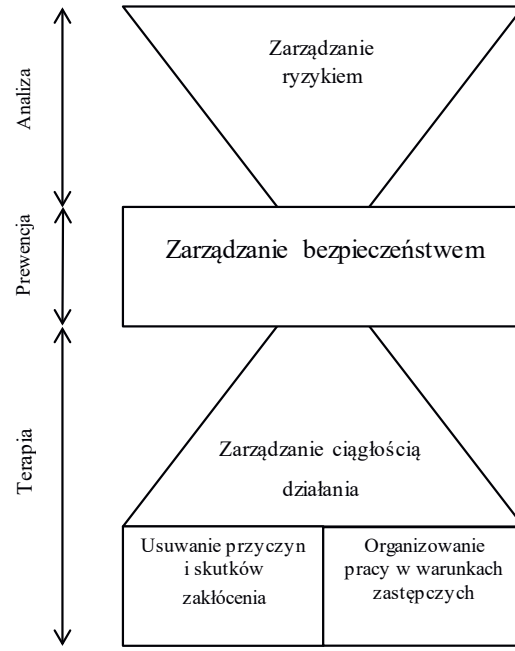
Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Nr procesu	*Komórka wiodąca*	*Proces*
	Planowanie	Uzgodnienie planu zarządzania kryzysowego ministra, kierownika urzędu centralnego
	Planowanie	Przygotowanie opinii do planu zarządzania kryzysowego wojewody
	Planowanie	Współpraca UE i NATO (MOL)
	Planowanie	Współpraca UE i NATO (planowanie NCRS)
	WPI	Informowanie publiczne o zdarzeniach i zagrożeniach
	WPI	Organizacja posiedzeń RZZK
	WOIK	Sporządzenie NPOIK
	WOIK	Sporządzenie wykazu IK
	WOIK	Identyfikacja EIK
	WOIK	Opiniowanie sprawozdań i raportów Pełnomocników IK (MSP)
	WOIK	Organizacja krajowego forum IK
	WOIK	Raportowanie do KE (dwuletnie; Dyrektywa 114)
	WOIK	Współpraca z UE i NATO w OIK (raportowanie do KE <roczne>)
	WOIK	Współpraca z UE i NATO w OIK (utrzymanie CIP PoC)
	WOIK	Współpraca z UE i NATO w OIK (CIWIN)
	WOIK	Współpraca z UE i NATO w OIK (opinie do dokumentów)
	WOIK	Zatwierdzanie planów ochrony IK
	WOIK	Sporządzenie listy osób kontaktowych dotyczących IK
	WOIK	Powoływanie Pełnomocników ds. OIK
	WOIK	Odwoływanie Pełnomocników ds. OIK
	WOIK	Opracowanie poradników z zakresu OIK
	WOIK	Przeprowadzenie szkolenia z zakresu OIK (materiały wybuchowe, dokumenty)
	Dyrektor	Świadczenie usług eksperckich (szkolenia, konferencje)
	Dyrektor	Świadczenie usług eksperckich (udział w innych ćwiczeniach niż zidentyfikowane powyżej)
	IT	Wystawianie i dystrybucja certyfikatów SNPI OPAL
	Sek. współpracy międzynarodowej	Koordynacja ćwiczeń CMX
	Sek. współpracy międzynarodowej	Sporządzanie wkładów do dokumentów NATO (w tym opiniowanie)
	Sek. współpracy międzynarodowej	Koordynacja przepływu informacji PL – NATO (CEPC i CPG)

Źródło: RCB, koncepcja planu ciągłości działania – materiał niepublikowany

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Ryzyko operacyjne można rozpatrywać nie tylko w kontekście prowadzonych na bieżąco procesów, ale również z perspektywy celu operacyjnego (bieżącego) działania organizacji (Zawiła-Niedźwiecki 2013). Ryzykiem tym można zarządzać, co sprowadza się do triady zagadnień: zarządzanie ryzykiem – zarządzanie bezpieczeństwem – zarządzanie ciągłością działania. Wymienionym elementom odpowiadają odpowiednio działania z zakresu analizowania, prewencji i terapii. Zależności pomiędzy omawianymi działaniami przedstawiono na schemacie nr 12.



Schemat 12. Zależności zadań zapewniania bezpieczeństwa i ciągłości działania
Źródło: Zawiła-Niedźwiecki 2013, s. 56

Aby zrozumieć istotę ryzyka operacyjnego w odniesieniu do realizacji bieżącego celu działania administracji publicznej, należy przeanalizować wzajemne powiązania pomiędzy tą administracją a systemem zarządzania kryzysowego. Wprawdzie ten system jest jednym z elementów administracji publicznej, ale realizuje odmienne cele. W efekcie ryzykiem operacyjnym dla administracji publicznej są zakłócenia w działaniach prowadzonych na rzecz ludności, podmiotów gospodarczych itp. Jednym z elementów zapewniających ciągłość działania administracji pomimo wystąpienia zakłócenia jest system zarządzania kryzysowego. Natomiast z punktu widzenia systemu zarządzania kryzysowego ryzykiem operacyjnym nie jest wystąpienie czynnika zakłócającego działanie administracji, lecz brak dostępu do zasobów niezbędnych, by przeprowadzić działania naprawcze. W efekcie można postawić tezę, że definicja ryzyka operacyjnego jest uzależniona od perspektywy, z której oceniamy cele, jakie administracja publiczna zamierza

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

osiągnąć. Dla administracji traktowanej całościowo (łącznie z zarządzaniem kryzysowym, które jest jej częścią) definicja ryzyka operacyjnego jest następująca.

Przez ryzyko operacyjne należy rozumieć ryzyko negatywnego oddziaływania na życie i zdrowie ludzi, mienie (w tym dziedzictwo kulturowe), środowisko naturalne, gospodarkę i infrastrukturę krytyczną oraz ryzyko strat materialnych i reputacyjnych, wynikających z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku procesu zmian w środowisku naturalnym, polityczno-militarnym i społeczno–kulturowym oraz w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych (Skomra 2017 b).

Dla systemu zarządzania kryzysowego traktowanego jako odrębna organizacja definicja ryzyka operacyjnego jest znacznie węższa i brzmi następująco.

Ryzyko operacyjne oznacza ryzyko strat materialnych i reputacyjnych oraz odpowiedzialności prawnej, wynikających z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych (Zawiła-Niedźwiecki 2013, s. 62).

Z uwagi na zakres niniejszego opracowania ta druga definicja została przyjęta za właściwszą. Dla wyjaśnienia tego paradoksu (dwie różne definicje tego samego pojęcia) posłużmy się przykładem. Awaria turbiny w elektrowni jest zdarzeniem niekorzystnym będącym zmaterializowaniem się ryzyka operacyjnego, jakie towarzyszy prowadzonej działalności. Brak właściwej reakcji na to zagrożenie może mieć poważny wpływ na uzyskiwane zyski i prowadzić do sytuacji kryzysowej. Dla firmy specjalizującej się w naprawie turbin ta sama awaria jest okazją do osiągnięcia zysków. Oczywiście procesowi naprawiania turbiny też towarzyszą różne rodzaje ryzyka operacyjnego. Są nimi np. brak dostępności niezbędnych części zamiennych, personelu itp. Awaria, która proces naprawy zapoczątkowała, jest z tej perspektywy jedynie szansą (ryzykiem pozytywnym).

Przez analogię, system zarządzania kryzysowego w przypadku wystąpienia zakłócenia ma za zadanie uruchomić rutynowe procesy naprawcze. Równolegle musi zarządzać ryzykiem operacyjnym, które mogłoby te procesy zakłócić. Aby zarządzać ryzykiem operacyjnym, z uwagi na zmienną strukturę systemu zarządzania kryzysowego (niektóre komórki uaktywniane są dopiero po wystąpieniu sytuacji kryzysowej, a ich skład osobowy zależy od rodzaju zagrożenia), podstawowym podejściem stosowanym do opisu zadań realizowanych przez system jest podejście procesowe. Przeszkodą uniemożliwiającą pełny opis procesów realizowanych w ramach systemu jest zmiana celów i form działania zarządzania kryzysowego wynikająca z konieczności wdrożenia nowych regulacji prawnych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

5.2. Zarządzanie reputacją i komunikacją kryzysową

Wśród różnych rodzajów ryzyka operacyjnego, które mogą oddziaływać na system zarządzania kryzysowego, nie można pominąć skutków związanych z utratą reputacji, a szerzej patrząc, skutków utraty zaufania. Na zagadnienie reputacji, której utrata może spowodować sytuację kryzysową, zaczęto zwraca uwagę po kryzysie nazywanym *Brent Spar*. W roku 1995 koncert Royal Dutch/Shell podjął racjonalną finansowo decyzję o zatopieniu na Morzu Północnym wyeksploatowanej wieży wiertniczej (a precyzyjniej boi magazynowej) *The Brent Spar*. Miejsce zatopienia wieży i sposób przeprowadzenia operacji miały zminimalizować oddziaływanie na środowisko naturalne, ale przede wszystkim firma miała zaoszczędzić na wydatkach związanych z holowaniem wieży do stoczni i jej pocięciem. Po tej decyzji konsumenci na całym świecie rozpoczęli bojkot produktów firmy, zaś organizacja Greenpeace przystąpiła do okupacji wieży. Dochodziło również do sytuacji drastycznych jak podłożenie ładunku wybuchowego pod stacją benzynową na terenie Niemiec. W efekcie koncern musiał się wycofać z podjętej decyzji, a straty spowodowane bojkotem konsumentów zostały oszacowane na kilkaset milionów dolarów (Schultz, Hatch, Larsen 2000).

Sytuacja, w której nie występuje żadne zagrożenie, a mimo to dochodzi do wymiernych strat finansowych, stała się początkiem nowego podejścia do komunikowania się pomiędzy organizacjami a ich otoczeniem. Najpierw w koncernie Shell, a później w innych organizacjach zarządzanie reputacją (*reputation management*) zaczęto traktować jako proces ciągły, w odróżnieniu od komunikacji ryzyka (*risk communication*), którą wprawdzie przygotowuje się wcześniej, ale z myślą o działaniach, jakie się podejmie po wystąpieniu sytuacji kryzysowej. To drugie podejście jest obecne w krajowym systemie kryzysowym (*Księga komunikacji kryzysowej*, 2017), a jego zakres jest oparty na kluczowych zasadach komunikacji kryzysowej określonych w normie Zarządzanie kryzysowe – wytyczne i dobre praktyki (BS 11200: 2014). Wykaz tych zasad przedstawiono w tabeli poniżej.

Tabela 24. Kluczowe zasady komunikacji kryzysowej

Lp.	*Nazwa zasady*	*Opis zasady*
	Bądź przygotowany	Przygotuj jasny i zrozumiały proces komunikacji
	Działaj szybko	Przekazuj informacje szybko i w odpowiedni sposób, podkreślając przy tym, że więcej informacji zostanie podanych, kiedy tylko to będzie możliwe
	Stale monitoruj	Koniecznie śledź wszystkie wydarzenia
	Utrzymaj przepływ informacji	Informuj o tym, co wiadomo; lepiej komunikować mało i często, niż czekać na możliwość opublikowania wszystkich informacji
	Mów jednogłośnie	Lecz niekoniecznie ustami jednego rzecznika
	Bądź otwarty i szczery	Wszystko i tak w końcu wyjdzie na jaw

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Lp.	*Nazwa zasady*	*Opis zasady*
	Rzetelność ma znaczenie	Operuj twardymi faktami, unikaj pogłosek, domysłów i przypuszczeń
	Przeproś	Kiedy to odpowiednie i istotne, nie bój się przeprosić
	Opracuj strategię	Określ podstawowy przekaz oraz tematy pomocnicze i rozwijaj je
	Zarządzaj terminami	Informuj w pierwszej kolejności najbliższych interesariuszy
	Bądź człowiekiem	Kiedy to właściwe, okazuj empatię
	Podpisz	Wiedz, kto ma kompetencje do zatwierdzania komunikatów do emisji.

Źródło: Abgarowicz 2015 na podstawie BS 11200:2014

Warunkiem powodzenia komunikacji ryzyka jest wcześniejsze uzyskanie wiarygodności w oczach przyszłych uczestników działań, a w szczególności osób, do których decydenci będą kierować niezbędne polecenia. Raz popełniony błąd w tej dziedzinie może skutkować przez wiele lat. Po awarii w Czarnobylu 26.04.1986 r. akcję informowania społeczeństwa i podawania dzieciom jodu rozpoczęto 29.04.1986 r., czyli z trzydniowym opóźnieniem (Jaworski 1996). Świadomość, że władza może ukrywać przed społeczeństwem tak istotne informacje, powoduje, że cyklicznie w Internecie pojawiają się „sprawdzone" informacje o rzekomej katastrofie elektrowni atomowej. Niekiedy powstawaniu takich plotek sprzyjają informacje rzeczywiste. W dniu 2.09.2017 pojawiły się informacje, że władze niemieckie podjęły decyzję o rozdaniu mieszkańcom terenów graniczących z Belgią tabletek z jodem. Decyzję motywowano złym stanem technicznych elektrowni Tihange[18]. Z uwagi na paniczne wykupowanie leków zawierających jod koniecznym było wystosowanie przez Polską Agencję Atomistyki komunikatu stwierdzającego brak zagrożenia i przeprowadzenie działań medialnych przestrzegających obywateli, by w trosce o własne zdrowie nie przyjmowali medykamentów z jodem. Sytuację uspokoiło dopiero pojawienie się w niezależnych mediach informacji potwierdzających, że rzekoma awaria to tylko plotka.

Nie zawsze fałszywa informacja jest dziełem internauty poszukującego swoiście pojmowanego rozgłosu. Dezinformacja wykorzystująca brak zaufania obywateli do własnych rządów stała się wręcz nową bronią o znaczeniu strategicznym (Darczewska 2017).

Niezależnie od celowego lub niecelowego wykorzystywania informacji do wywoływania niepokojów społecznych brak lub ograniczone zaufanie obywateli do swoich władz może mieć bezpośredni wpływ na przebieg działań podczas sytuacji kryzysowych. Jak dowodzi S. Schneider (Schneider 1995) w celu skutecznego

[18] Komunikat PAA z dnia 2.09.2017, http://www.paa.gov.pl/aktualnosc-305-komunikat_w_elektrowni_tihange_w_belgii.html [dostęp: 20.12.2017].

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

prowadzenia działań administracja przygotowuje normy o charakterze biurokratycznym, które obejmują wszystkich uczestników działań, łącznie z mieszkańcami, którzy powinni zachować się w ściśle określony sposób. Obowiązuje przy tym zasada, że działania bezpośrednio dotykające ludzi (ewakuacja, utrzymanie minimalnych warunków bytowych) powinny być przeprowadzane na szczeblu lokalnym. W czasie sytuacji kryzysowej pod presją zagrożenia pomiędzy oczekiwaniami społeczeństwa a normami biurokratycznymi pojawia się rozdźwięk (autorka używa określenia „gaps"). Ten rozdźwięk jest warunkowany następującymi czynnikami:

- rozmiar katastrofy,
- stopień przygotowania władz publicznych,
- postrzeganie zagrożenia przez społeczność.

Jeśli luka jest niewielka, władze cieszą się zaufaniem społecznym, działania uczestników były dobrze zaplanowane, zaś potrzeby ratowanych uwzględnione sytuacja, jest postrzegana jako poprawna, zaś wysiłki władz są uważane za sukces. Reagowanie, koordynacja i wsparcie przebiegają w relacjach „z dołu do góry". Rozdźwięk przybiera średnie rozmiary, jeśli działania są źle przygotowane, akcja jest prowadzona chaotycznie, poszczególne działania nie są koordynowane, ale nie są ze sobą sprzeczne. Pod naciskiem opinii publicznej pojawia się model mieszany. Władze wyższego szczebla próbują wpłynąć na niekorzystny przebieg działań, wprowadzając nieplanowane elementy koordynacji regionalnej lub centralnej. W najgorszym przypadku normy biurokratyczne zawodzą (lub nigdy ich nie było), a uczestnicy są zmuszani do działań niestandardowych. W efekcie działanie „z dołu do góry" jest zastępowane wymuszonym działaniem „z góry do dołu". Taka sytuacja nigdy nie jest odbierana jako sukces. Wymuszony presją społeczną proces przekazywania odpowiedzialności pomiędzy poszczególnymi poziomami administracji nie jest procesem łatwym, a ponadto sam w sobie niesie dodatkowe problemy. Po pierwsze, już sama możliwość przekazania odpowiedzialności na wyższy szczebel ogranicza determinację władz lokalnych do samodzielnego uporania się z powstałą sytuacją. Tym bardziej, gdy przekazaniu odpowiedzialności towarzyszy możliwość pozyskania dodatkowych środków. Wówczas władze lokalne mogą wręcz świadomie opóźniać lub ograniczać własne działania, chcąc w ten sposób zmusić wyższe szczeble administracji do przejęcia zarządzania sytuacją i wydatkowania na nie własnych środków. Władze centralne też nie wykazują entuzjazmu do przejmowania odpowiedzialności od władz lokalnych. Władze centralne boją się zarzutów o przekroczenie własnych kompetencji. Personel administracji centralnej zwykle nie jest przygotowany do wykonywania funkcji sprawowanych normalnie przez władze lokalne. Nie znają też uwarunkowań lokalnych i kondycji finansowej władz niższego szczebla. Poszczególne agencje centralne mają również problemy z koordynacją działań pomiędzy sobą. W efekcie zdaniem S. Schneider, opóźnienie z podjęciem działania, problemy koordynacyjne

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

i niedostosowanie działań do uwarunkowań lokalnych, to wręcz charakterystyczne cechy działania władz centralnych.

Dla porządku należy dodać, że nie zawsze postawy uczestników zdarzenia wobec pojawiającego rozdźwięku pomiędzy oczekiwaniami a normami biurokratycznymi mają charakter negatywny. Poza krytyką władz poszkodowani często biorą sprawy w swoje ręce i angażują się w działania. Przykładowo podczas huraganu, jaki miał miejsce 11.08.2017 r. w rejonie Chojnic, mieszkańcy nie mogąc doczekać się pomocy ze strony władz, sami usuwali zatory na drogach oraz na rzece Brdzie. W najbardziej skrajnym przypadku może jednak dojść do samoorganizacji ludzi przeciwko władzom, co uniemożliwi dalsze prowadzenie działań.

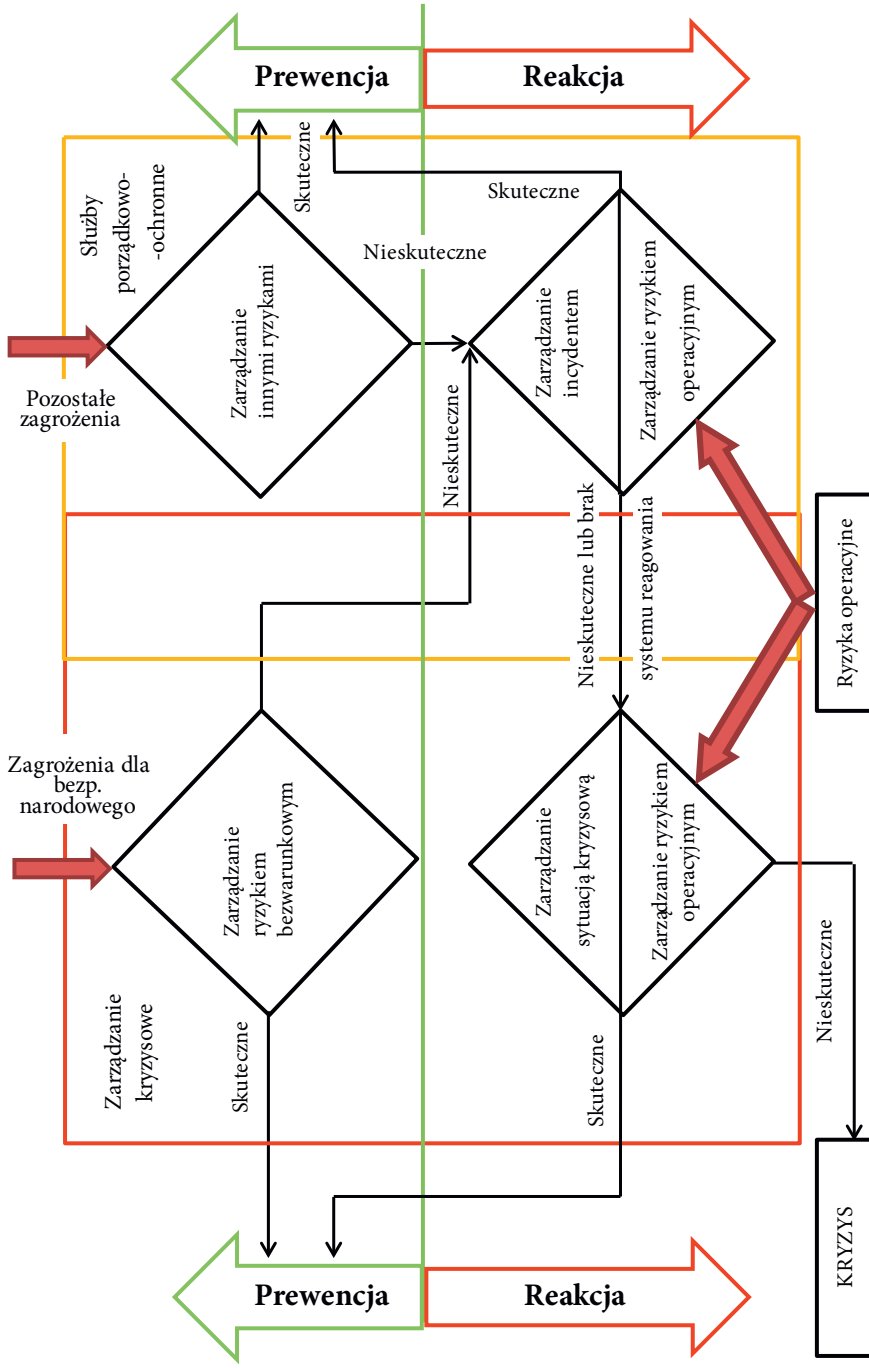
Podsumowując należy podkreślić, że rozdźwięk pomiędzy oczekiwaniami społecznymi a normami biurokratycznymi przygotowanymi na czas sytuacji kryzysowych może stanowić o pojawieniu się dodatkowego ryzyka operacyjnego.

Warunkiem uniknięcia takiej sytuacji jest nie tylko właściwe planistyczne i techniczne przygotowanie działań, ale włączenie ludności w proces budowania bezpieczeństwa oparty na wzajemnym zaufaniu. Komunikowanie o właściwej reakcji w momencie gdy woda wlewa się do domu, nigdy nie będzie uznane za właściwe. Informowanie o planowanych działaniach, przygotowanie ludności na możliwe zagrożenia, transparentność w polityce informacyjnej oraz właściwa komunikacja ryzyka są elementami, które zwiększają lub zmniejszają możliwość pojawienia się rozdźwięku między oczekiwaniami społecznymi a zamierzeniami władz. To z kolei przekłada się na poziom ryzyka operacyjnego.

5.3. Zintegrowane zarządzanie ryzykiem w ramach zarządzania kryzysowego

Trudność w opisie rodzajów ryzyka operacyjnego w odniesieniu do zarządzania kryzysowego spowodowana jest również trwającym procesem zmiany. System, który skupiał się na fazie reakcji, powinien szerzej wdrażać działania z zakresu zapobiegania zagrożeniom dynamicznym (zagrożenia statyczne, których miarą są ryzyka odłożone, nie wchodzą w zakres podmiotowy zarządzania kryzysowego). Aby osiągnąć cel główny, system zarządza (lub powinien zarządzać) ryzykiem bezwarunkowym, podatnością oraz ryzykiem warunkowym. Procesowi zarządzania różnymi rodzajami ryzyka towarzyszy ryzyko operacyjne. Zarządzanie ryzykiem warunkowym, w powiązaniu z ryzykiem operacyjnym, jest związane z możliwością wystąpienia sytuacji kryzysowej. Taka sytuacja to wskaźnik, którego pojawienie się oznacza konieczność podjęcia działań naprawczych. Przebieg działań prowadzonych w celu zarządzania obu rodzajami ryzyka przedstawiono na schemacie nr 13.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353



Schemat 13. Zarządzanie ryzykiem bezwarunkowym i warunkowym w ramach systemu zarządzania kryzysowego

Źródło: opracowanie własne

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zarządzanie obu rodzajami ryzyka różni się celem działania, sposobami osiągania celu oraz podejściem. Wykaz tych różnic przedstawiono w tabeli nr 25.

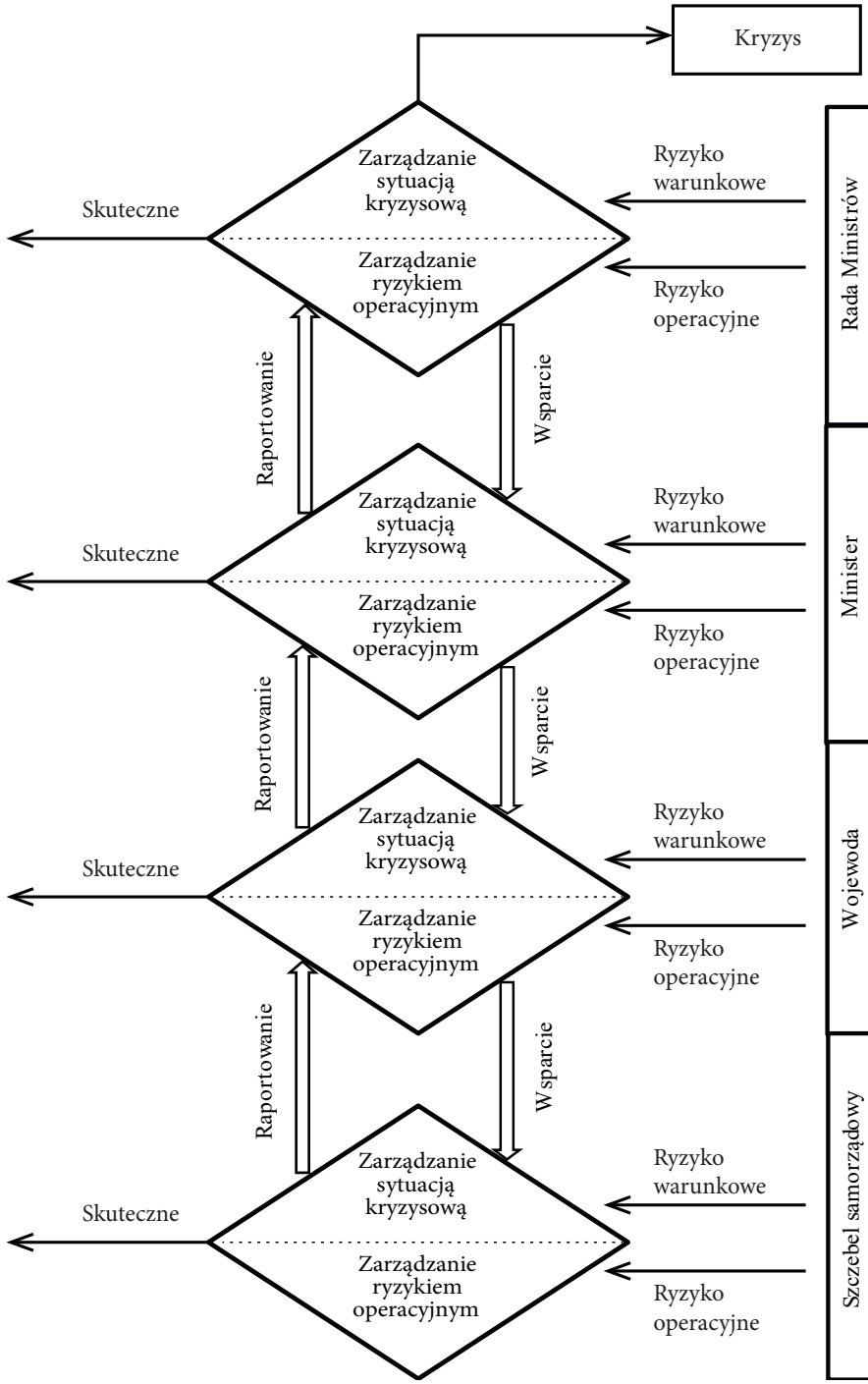
Tabela 25. Zarządzanie ryzykiem w ramach systemu zarządzania kryzysowego

	Zarządzanie ryzykiem bezwarunkowym	*Zarządzanie sytuacją kryzysową*	
		Zarządzanie ryzykiem warunkowym	Zarządzanie ryzykiem operacyjnym
Cel	Minimalizacja ryzyka związanego z zidentyfikowanym zagrożeniem	Minimalizacja ryzyka związanego z możliwością wystąpienia sytuacji kryzysowej (zagrożenia warunkowego)	Minimalizacja ryzyka związanego z zawodnością podmiotów, służb i systemów administracji publicznej powołanych do zwalczania zagrożeń
Sposób osiągania celu	– usunięcie źródła zagrożenia; – zmniejszanie prawdopodobieństwa wystąpienia; – zbudowanie barier suplementowych poprzez zmniejszanie podatności obiektów i obszarów (zmniejszanie podatności ze względu na przyczynę)	– budowanie barier systemowych, tj. systemów ratowniczych i ochronnych adekwatnie do poziomu ryzyka; – stałe przygotowanie i doskonalenie administracji i służb ratowniczych do działań wykraczających poza rutynowe reagowanie; – zgromadzenie niezbędnych zasobów; – zbudowanie barier suplementowych poprzez zmniejszanie podatności obszarów i społeczności (zmniejszanie podatności ze względu na skutek)	– zapewnienie ciągłości działania administracji i służb ratowniczych w razie wystąpienia ryzyka operacyjnego; – zapewnienie wsparcia, tj. uruchomienie działań organizacyjnych, technicznych oraz zapewnienie dodatkowego finansowania pozwalającego przywrócić prawidłowe funkcjonowanie administracji i służb.
Stosowane podejście	Głównie projektowe, wspomagająco procesowe	Głównie procesowe, wspomagająco projektowe	Procesowe

Źródło: opracowanie własne

System, aby osiągnąć cel główny i cele pośrednie, realizuje wiele procesów. Procesy przebiegają pomiędzy elementami systemu a jego otoczeniem oraz pomiędzy elementami systemu (na jednym poziomie administracyjnym i pomiędzy poziomami). Przebieg procesów wewnętrznych w ramach zarządzania sytuacją kryzysową przez podmioty systemu przedstawiono na schemacie nr 14.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353



Schemat 14. Przepływ informacji i zasobów w ramach zarządzania sytuacją kryzysową
Źródło: opracowanie własne

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Symptomem wystąpienia sytuacji kryzysowej jest pojawienie się poważnych zakłóceń w działalności administracji publicznej będących następstwem nieadekwatności posiadanych sił i środków w porównaniu do wielkości bądź charakteru zagrożenia. Ze względu na strukturę hierarchiczną system może znajdować się jednocześnie w różnych stanach na poszczególnych poziomach. Przykładowo na szczeblu samorządowym wystąpiła sytuacja kryzysowa, szczebel wojewódzki (w jednym lub kilku województwach) został aktywowany w związku z możliwością wystąpienia sytuacji kryzysowej, zaś szczebel centralny jedynie monitoruje sytuację. Możliwe są również sytuacje odwrotne, kiedy to sytuacja kryzysowa występuje na szczeblu centralnym, zaś szczebel samorządowy realizuje jedynie zadania z obszaru monitorowania zagrożeń.

Podejmowane działania korekcyjne związane z wystąpieniem lub możliwością wystąpienia sytuacji kryzysowej to zarządzanie sytuacją kryzysową obejmujące zarządzanie ryzykiem warunkowym i jednocześnie ryzykiem operacyjnym. Celem tych działań (cel pośredni systemu zarządzania kryzysowego) jest utrzymanie na minimalnym akceptowalnym poziomie sprawności administracji (w tym służb, inspekcji i straży) oraz uruchomienie środków technicznych, rozwiązań organizacyjnych oraz zasobów materiałowych i finansowych przywracających akceptowalny poziom skuteczności jej funkcjonowania. Zarządzanie sytuacją kryzysową kończy się w momencie, gdy utrzymanie poziomu bezpieczeństwa wymaga jedynie rutynowych działań służb, inspekcji i straży odpowiedzialnych za minimalizowanie skutków zagrożenia. Wystąpienie sytuacji kryzysowej dla administracji publicznej jest symptomem niewłaściwego stanu organizacji. Jednak z perspektywy systemu zarządzania kryzysowego jest to jedynie okoliczność powodująca konieczność uruchomienia rutynowych procedur.

W teorii zarządzania ryzykiem wyróżnia się pięć etapów zarządzania ryzykiem (Szlachcic 2014):

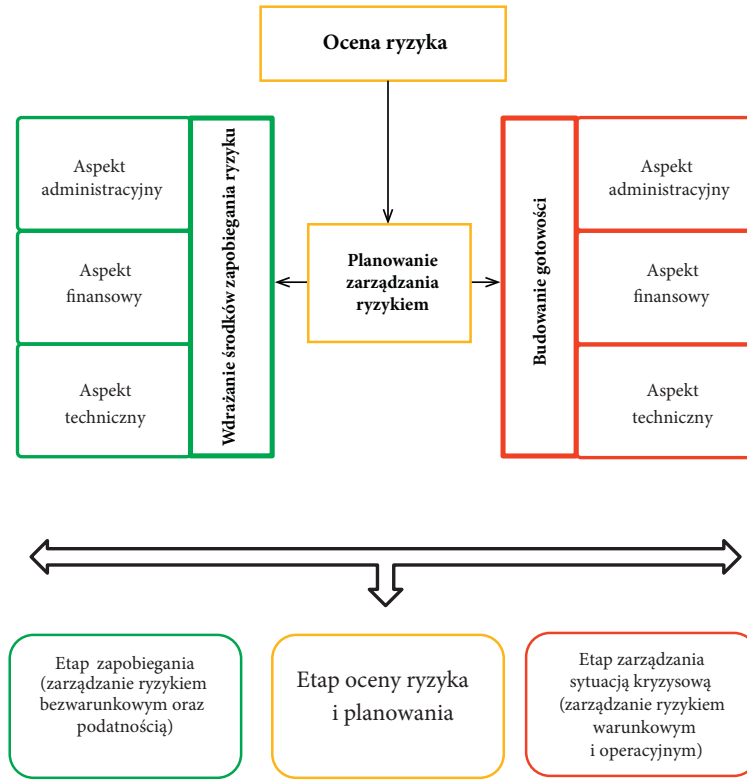
- etap I – identyfikacja i analiza konsekwencji, które mogłyby spowodować stratę;
- etap II – określenie alternatywnych metod zarządzania ryzykiem;
- etap III – wybór optymalnej metody zarządzania ryzykiem;
- etap IV – zastosowanie wybranej metody;
- etap V – monitorowanie wyników.

Nowe uwarunkowania prawne wynikające z UMOL powodują, że system powinien osiągnąć zdolność zarządzania ryzykiem. W ramach tego zadania zdefiniowano cztery zasadnicze etapy. Są nimi:

- ocena ryzyka,
- planowanie zarządzania ryzykiem,
- zapobieganie ryzyku,
- zapewnienie gotowości.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Wszystkie kroki tak zdefiniowanego procesu powinny być rozpatrywane w trzech aspektach, tj. finansowym, administracyjnym i technicznym. Decyzja nie określa, jak poszczególne zadania są ze sobą powiązane ani jak powinien wyglądać cykl postępowania z ryzykiem. Na bazie przeprowadzonych badań, uwzględniając odmienność podejścia do ryzyka bezwarunkowego i warunkowego, można zaproponować następujący schemat obrazujący kolejność niezbędnych działań.



Schemat 15. Etapy osiągania zdolności zarządzania ryzykiem
Źródło: opracowanie własne na podstawie: Skomra 2017 c, s. 246

Przedstawiony schemat, w zakresie wskazania procedury działania, jest komplementarnym uzupełnieniem schematu nr 8 przedstawiającego model funkcjonalno-strukturalny systemu bezpieczeństwa z uwzględnieniem ryzyka warunkowego i bezwarunkowego. Oba schematy łącznie stanowią autorski model zależności pomiędzy bezpieczeństwem narodowym a zarządzaniem kryzysowym łączący strukturę organizacyjną z procedurą postępowania administracji publicznej wobec wystąpienia zagrożeń dla ludności. Zaproponowane w modelu rozdzielenie procesu osiągania zdolności zarządzania ryzykiem na dwa podprocesy połączone ze sobą etapem oceny i planowania ma swoje uzasadnienie. Zapobieganie ryzyku (prewencja) dotyczy ryzyka bezwarunkowego oraz podatności. Budowanie gotowości na

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

wypadek wystąpienia sytuacji kryzysowej odnosi się natomiast do ryzyka warunkowego (wraz z towarzyszącym mu ryzykiem operacyjnym), które można rozpatrywać jedynie wówczas, gdy założymy, że zmaterializowało się pewne wcześniejsze ryzyko. W przypadku powodzi zarządzanie ryzykiem pierwotnym jest głównie zadaniem ministra właściwego do spraw środowiska i polega na ograniczeniu prawdopodobieństwa wystąpienia zjawiska oraz zmniejszeniu poziomu podatności poprzez właściwą gospodarkę wodną, planowanie przestrzenne itp. Zarządzanie ryzykiem warunkowym, polegającym na możliwości wystąpienia sytuacji kryzysowej, mieści się głównie w zakresie kompetencji ministra spraw wewnętrznych i administracji, a polega na budowaniu barier systemowych (struktury reagowania, systemy ratownicze, zasoby materiałowe itp.) oraz barier suplementowych (budowanie świadomości zagrożeń wśród społeczności narażonej na ryzyko powodziowe, wspieranie procesu samoorganizacji itp.) (Skomra 2015). Upraszczając – niezależnie od zawodności barier suplementowych i systemowych, bez zmaterializowania się ryzyka bezwarunkowego sytuacja kryzysowa związana z nieskutecznością systemów reagowania nie zaistnieje. Oczywiście poprawa skuteczności barier zmniejsza ryzyko wystąpienia sytuacji kryzysowej, ale nie wpływa na ilość powodzi. Trudno zatem takie działanie zaliczyć do fazy zapobiegania. Tym, co różni zarządzanie ryzykiem bezwarunkowym od warunkowego, jest również inna perspektywa czasowa. Zarządzanie ryzykiem bezwarunkowym odbywa się w perspektywie średnio- i długoterminowej (5 do 10 lat lub dłużej) na podstawie dokumentów strategicznych lub programów (np. NPOIK). Zarządzanie ryzykiem warunkowym dotyczy perspektywy krótko- i średnioterminowej (2 do 5 lat) oraz opiera się na dokumentach operacyjnych lub programach (np. Krajowy Plan Zarządzania Kryzysowego, Program modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Biura Ochrony Rządu w latach 2017–2020 (DzU 2016 r. poz. 2140)).

Jednocześnie, jak dowodzą badania prowadzone w ramach projektu „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego”[19], ryzyko, nad którym administracja musi panować, powinno być postrzegane w następujących trzech aspektach:

- ryzyko bezpośrednio związane z wystąpieniem zakłóceń,
- ryzyko wystąpienia sytuacji kryzysowej,
- ryzyko strat finansowych na skutek nietrafnej decyzji co do podejmowanych działań zaradczych.

Dla każdego z powyższych aspektów istnieje inny sposób wyliczania ryzyka. Dla ryzyka bezpośrednio związanego z wystąpieniem zakłócenia jest to wzajemna

[19] Projekt nr DOBR/0077/R/ID3/2013/03 finansowany przez NCBiR realizowany przez Konsorcjum: Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Medcore Sp. z o.o., Szkoła Główna Służby Pożarniczej, Wydział Bezpieczeństwa Akademii Obrony Narodowej (obecnie Akademia Sztuki Wojennej), Wydział Zarządzania Politechniki Warszawskiej. Autor jest kierownikiem tego projektu.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

korelacja prawdopodobieństwa zdarzenia i jego skutków (ewentualnie prawdopodobieństwa, podatności i spodziewanych skutków). Dla ryzyka wystąpienia sytuacji kryzysowej jest to korelacja wielkości posiadanych zasobów z prawdopodobieństwem wystąpienia zdarzenia tak dotkliwego, że zasoby te okażą się niewystarczające. Wreszcie, ryzyko strat finansowych w przypadku podjęcia nietrafnych decyzji, które należy kalkulować, stosując teorię gier. Niezależnie od powyższych aspektów system zarządzania kryzysowego narażony jest na ryzyko operacyjne. Zagrożenia generujące ryzyko wystąpienia sytuacji kryzysowej zostaną omówione w dalszej części.

5.4. Elementy ekonomiki w zarządzaniu ryzykiem i niepewnością

Pojęcia „ryzyko" i „niepewność" kształtowały się w naukach ekonomicznych już na początku XX w., choć obu określeń używano już wcześniej. Proces kształtowania się obu pojęć można prześledzić na kilku przykładach. Już w 1901 r., w pracy *The Economic Theory of Risk and Insurance* (Willetta 2002), autor twierdził, że stopień niepewności nie jest zbieżny ze stopniem prawdopodobieństwa, gdyż w miarę jak zwiększa się prawdopodobieństwo, następuje zmniejszenie się niepewności. Z kolei w 1921 r. ukazała się rozprawa (Knight 2012), gdzie autor stwierdził, że pojęć „niepewności" i „ryzyka" nie należy utożsamiać. Niepewność dotyczy zdarzeń (zjawisk) o charakterze jakościowym. Ryzyko odnosi się do zdarzeń faktycznie zachodzących. Inną cechą ryzyka jest jego powiązanie ze zdarzeniami negatywnymi (np. ryzyko straty), tymczasem niepewność może się odnosić również do zdarzeń pozytywnych (np. niepewność zysku). Podsumowując swoje rozważania, Knight uznał niepewność za niemierzalną, w przeciwieństwie do mierzalnego ryzyka. W tym samym nurcie utrzymane są wnioski zawarte w pracy (Jedynak, Szydło 1997). Autorzy ryzyko zaliczyli do zjawisk częstych, niepewność – do powszechnych. Ponadto niepewność jest pojęciem szerszym, ryzyko – węższym. Ryzyko, jako powiązane z działalnością człowieka, ma charakter dynamiczny. Niepewność natomiast takiej cechy nie posiada. Ryzyko jest związane zarówno z możliwością uzyskania korzyści, jak i poniesienia straty. Podejmowanie ryzyka często kojarzy się ze zjawiskiem pozytywnym. Natomiast podejmowanie działań w warunkach niepewności jest utrudnione, stąd przypisuje się jej charakter negatywny lub obojętny. Najważniejszym stwierdzeniem prowadzonych rozważań jest stwierdzenie, iż istnieje cecha wspólna ryzyka i niepewności. Zdaniem autorów niepewność jest przyczyną ryzyka.

Pomimo że niepewność jest kategorią niemierzalną, podejmowano próby racjonalizacji podejmowania decyzji również w takich sytuacjach z uwzględnieniem kryteriów, jakimi posługuje się decydent. M. Bochenek (Bochenek 2012) wymienia następujące kryteria:

1. Kryterium Laplace'a, czyli największej nadziei matematycznej. Podmioty podejmujące decyzję nie mają informacji o prawdopodobieństwie wystąpienia

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

możliwych stanów natury, co oznacza, że każdy stan jest tak samo prawdopodobny. Do każdego wariantu działania można przyporządkować wielkość spodziewanego zysku. Podmiot wybiera i realizuje wariant, który zapewnia największy poziom zysku, czyli największą nadzieję matematyczną.

2. Kryterium Walda, czyli maksyminu. Spośród możliwych wariantów podmiot gospodarczy wybiera ten, który zapewnia najlepsze minimum. Oznacza to, że ze zbioru najgorszych rezultatów, czyli skrajnie niekorzystnych stanów natury, decydent wybiera najkorzystniejszy wynik. W kryterium Walda uwzględnia się więc możliwość realizacji przedsięwzięcia w najmniej sprzyjających okolicznościach.
3. Kryterium Savage'a, czyli minimaksu. Ocena wyboru w tym kryterium dotyczy skutków błędnej decyzji. Podmiot wybiera ten wariant, którego realizacja pociąga najmniejszą z maksymalnych strat. Wybór pada więc na najmniej niebezpieczne przedsięwzięcie.
4. Kryterium Bayesa, czyli wartości oczekiwanej. Spośród jednakowo prawdopodobnych stanów natury podmiot wybiera wariant, który zapewnia największą wartość oczekiwaną. Wybrany wariant pozwala więc zmaksymalizować produkcję lub inną wielkość.
5. Kryterium Hurwicza, czyli wskaźnika optymizmu. Podmiot decyzyjny uwzględnia w swoim działaniu jednocześnie wyniki najlepsze i najgorsze. Biorąc pod uwagę własne preferencje, decydent przewiduje wystąpienie sytuacji optymistycznej i pesymistycznej. Stosując strategię kompromisową, podmiot wybiera albo wariant maksymaksowy, albo wariant maksyminowy.

Aby wybrać właściwe kryterium należy zauważyć, że administracja publiczna nie działa z chęci zysku, ani nie optymalizuje swoich działań, kierując się spodziewanymi dochodami. Z tego powodu do jej działań w warunkach niepewności należy stosować kryterium Savage'a. W praktyce stosowanie kryterium sprowadza się do działań na tzw. matrycy żalu (Jędrzejczyk, Skrzypek, Kukuła (red.), Walkosz 2012). Adaptacja matrycy żalu do wykorzystania przez administrację publiczną została przeprowadzona w ramach projektu „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP" (Skomra 2015). Jej zastosowanie można przedstawić na następującym przykładzie. Nie wiemy, czy kolejna zima będzie ostra, czy łagodna. Mamy zatem następujące możliwości:

– nie wystąpią na tyle silne mrozy, aby jakiekolwiek działania były potrzebne;
– wystąpią mrozy na tyle silne, że pewne przedsięwzięcia należy poczynić, aby zmniejszyć ich skutki;
– wystąpią mrozy o dosyć istotnym nasileniu i należy się do nich solidnie przygotować;

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

– wystąpią mrozy ekstremalne, więc działania obniżające ryzyko z nimi związane powinny mieć poważny (kosztowny) charakter.

Te cztery scenariusze możemy określić następująco. W pierwszym przypadku jest to „brak zagrożenia", dla przypadku drugiego „małe zagrożenie", dla przypadku trzeciego „średnie zagrożenie", dla przypadku czwartego „duże zagrożenie". Jednak w przypadku innych zagrożeń lepiej się posługiwać prawdopodobieństwem, np. prawdopodobieństwem, że pewna ilość osób zapadnie na chorobę zakaźną. Może to być następująca skala: zerowe prawdopodobieństwo, małe, średnie lub duże.

Reakcja na spodziewane zagrożenie może być następująca:

1. Nic nie robić (realizowana jest rutynowa praca służb, straży i inspekcji),
2. Mała interwencja (np. zwiększenie częstotliwości monitorowania zagrożenia, wzmocnienie obsad osobowych podmiotów zajmujących się zagrożeniem).
3. Średnia interwencja (wzmocnienie gotowości podległych sił i środków, wstrzymanie urlopów, koncentracja przynajmniej części zasobów w wyznaczonych miejscach, zapewnienie gotowości udzielenia wsparcia przez inne podmioty do realizacji zdefiniowanych zadań).
4. Duża interwencja oznacza sięgnięcie po środki nadzwyczajne, mogące wpłynąć na płynność finansową podmiotu, np.: związane z wprowadzeniem stanu nadzwyczajnego z uwagi na niewystarczający charakter zwykłych środków.

Dla każdego z tych przypadków budujemy tabelę kosztów, zakładając, że średnia interwencja powinna obniżyć straty końcowe o ok. 50%, zaś duża o ok. 90% (ilość rodzajów reakcji można zwiększać lub zmniejszać w zależności od posiadanych danych). Budując tabelę kosztów, należy uwzględniać zarówno środki wydatkowane na minimalizację przyszłych strat, jak i same straty. Koszty przedstawiamy bezpośrednio w pieniądzu. Przykładowy wynik przedstawiono w tabeli nr 26.

Tabela 26. Przykładowa tabela kosztów w 1000 PLN przy różnych wariantach reakcji dla wszystkich możliwych wielkości zagrożeń

DZIAŁANIE	*Wielkość zagrożenia*			
	Znikomo małe	*Małe*	*Średnie*	*Duże*
Nie robić nic	10	20	40	70
Mała interwencja	11	20	45	71
Średnia interwencja	13	21	38	65
Duża interwencja	21	24	37	57

Źródło: Bralewski A., Piec R., Wróbel R., Opracowanie wzorcowego scenariusza zagrożenia zgodnie z metodyką zaimplementowaną w narzędziu ARMOR, materiał opracowany w ramach projektu „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP" (projekt nr O ROB/0077/03/003), SGSP 2016 r., s. 35

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

W kolejnym kroku tabelę kosztów przekształcamy w matrycę żalu. Przekształcenie polega na odszukaniu najmniejszych wartości poniesionych kosztów w poszczególnych kolumnach i odjęciu tej wartości od wartości kosztów zdefiniowanych w każdym polu tabeli kosztów. Uzyskaną w ten sposób matrycę przedstawiono w tabeli nr 27.

Tabela 27. Matryca żalu

DZIAŁANIE	*Wielkość zagrożenia*			
	Znikomo małe	*Małe*	*Średnie*	*Duże*
Nie robić nic	0	0	3	13
Mała interwencja	1	0	8	14
Średnia interwencja	3	1	1	8
Duża interwencja	11	4	0	0

Źródło: Bralewski A., Piec R., Wróbel R., Opracowanie wzorcowego scenariusza zagrożenia zgodnie z metodyką zaimplementowaną w narzędziu ARMOR, materiał opracowany w ramach projektu „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP" (projekt nr O ROB/0077/03/003), SGSP 2016 r., s. 36

Kolejnym krokiem jest wybór ze sporządzonej matrycy żalu wartości największej możliwej straty w ramach decyzji danego rodzaju (maksymalna wartość w każdym wierszu). Otrzymane kolejno wartości kosztów to:

- dla strategii „nic nie robić" – 13,
- dla strategii „mała interwencja" – 14,
- dla strategii „średnia interwencja" – 8,
- dla strategii „duża interwencja" – 11.

Ponieważ naszym celem jest ograniczenie do minimum strat w przypadku podjęcia nietrafionej decyzji, spośród zaprezentowanych czterech wartości kosztów wybieramy wartość 8, co oznacza, że optymalnym rozwiązaniem w tym przypadku jest reakcja na poziomie „średniej interwencji". Można ją zinterpretować w następujący sposób. Jeżeli nie trafimy z właściwą decyzją, to straty, jakie poniesiemy, i tak będą najniższe z możliwych. Jest to dla decydentów dobre uzasadnienie na wypadek zarzutów o marnowanie środków pochodzących z podatków.

W przeciwieństwie do niepewności ryzyko jest kategorią mierzalną. Celem obliczenia wartości ryzyka najczęściej stosowany jest wzór ilościowy zaproponowany przez stowarzyszenie FERMA (FERMA, Standard zarządzania ryzykiem, 2003).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Wyraża się on następująco:

R = P * S

R – ryzyko,

P – prawdopodobieństwo,

S – możliwe skutki oraz ich ciężkość.

Metodą służącą do oceny ryzyka katastrofalnego jest jakościowa metoda Risk Score, uwzględniająca ekspozycję, czyli czas trwania zakłócenia (Fine 1971). Wyraża się ona wzorem:

R = P * E * S

gdzie:

R – ryzyko,

P – prawdopodobieństwo,

E – czas ekspozycji na czynnik niebezpieczny,

S – możliwe skutki oraz ich ciężkość.

Wykorzystanie metody jakościowej związane jest z koniecznością uwzględnienia szeregu elementów towarzyszących ryzyku, które to elementy nie zawsze pozwalają stosować metody ilościowe. Przykładowo, poszukując cech ryzyka, B. Hadyniak (Hadyniak 2010) uznał, że ryzyko wiąże się wyłącznie z przyszłymi zdarzeniami i skutkami, które ze względu na znaczenie mogą zmienić ludzkie życie; występuje brak możliwości przewidzenia (niepewność) zdarzeń i skutków w przyszłości; wreszcie dotyczy wartości, które ludzie chcą zdobyć lub utrzymać. Z kolei J. Monkiewicz (Monkiewicz 2004) określił następujące cechy ryzyka:

- jest ono niejednorodne,
- jest zarówno w ujęciu subiektywnym, jak i obiektywnym,
- może być postrzegane w różnych kontekstach,
- jest zmienne i podlega wielu czynnikom,
- jest bardziej procesem niż stanem.

W odniesieniu do ryzyka związanego z funkcjonowaniem organizacji ryzyko powinno być postrzegane z uwzględnieniem jej otoczenia (J. Zawiła-Niedźwiecki 2013) można wyróżnić następujące przypadki:

- przyczyna w otoczeniu, skutek wewnątrz organizacji;
- przyczyna i skutek wewnątrz organizacji;
- przyczyna w organizacji, skutek w otoczeniu;
- przyczyna i skutek w otoczeniu.

W efekcie przytoczone wzory pozwalające wyliczyć lub ocenić ryzyko należy traktować wyłącznie jako przykładowe. W praktyce zastosowanie konkretnej metody pomiaru jest uzależnione od kontekstu, w jakim dokonuje się oceny ryzyka (Wróblewski red. 2015; Kosieradzka, Zawiła-Niedźwiecki 2016; Abgarowicz red. 2015; W. Skomra 2015).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zagadnieniem pochodnym w stosunku do pomiaru ryzyka jest obliczenie lub przynajmniej oszacowanie wpływu nakładów na redukowanie ryzyka (inwestycje w bezpieczeństwo) na przyszłe wyniki ekonomiczne. Tego typu rozważania zawsze napotykają na podstawową trudność. Nakłady na poprawę bezpieczeństwa są pewne i natychmiastowe, a ewentualne zyski trudne do oszacowania i odłożone w czasie. Metodę oszacowania zysków z zastosowanych inwestycji w bezpieczeństwo zaproponowała Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA 2012). Wprawdzie metodyka dotyczy optymalizowania nakładów na bezpieczeństwo teleinformatyczne, ale ze względu na uniwersalny charakter może być stosowana również w innych obszarach.

Metodyka polega na obliczeniu zwrotu z inwestycji w bezpieczeństwo ROSI (*Return on Security Investment*) przy wykorzystaniu następujących danych wyjściowych:

- **Kb** – korzyści (wyrażone w pieniądzach) z wdrożenia danego rozwiązania z zakresu bezpieczeństwa;
- **Nb** – nakłady (wyrażone w pieniądzach) na wdrożenie danego rozwiązania z zakresu bezpieczeństwa;
- **ALE** – oczekiwana roczna strata (**ALE – *Annual Loss Expentancy***) – straty (wyrażone w pieniądzach), jakie możemy potencjalnie ponieść w ciągu roku;
- **Wzm** – współczynnik zmniejszenia ryzyka – oczekiwana redukcja ryzyka w wyniku wprowadzenia danego rozwiązania podniesienia bezpieczeństwa;
- **SLE –** oczekiwana jednorazowa strata (**SLE – *Single Loss Expectancy*) –** strata (wyrażona w pieniądzach) z jednego incydentu bezpieczeństwa;
- **ARO** – roczny współczynnik wystąpienia (**ARO – *Annual Rate of Occurence***) – jest miarą prawdopodobieństwa, że dane ryzyko występuje w ciągu roku.

$$ROSI = \frac{Kb - Nb}{Nb} \times 100\%$$

$$Kb = ALE \times Wzm$$

$$ALE = SLE \times ARO$$

$$ROSI = \frac{SLE \times ARO \times Wzm - Nb}{Nb}$$

Przykład (na podstawie: Pyznar 2017)[20]. Firma A rozważa obniżenie ryzyka związanego z utratą danych na skutek działania wirusów komputerowych. Dane statystyczne wskazują, że porównywalne przedsiębiorstwa doświadczają 5 ataków

[20] Autor przykładu posłużył się wartościami wyrażanymi w euro, ale metoda może być zastosowane dla każdej waluty.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

rocznie (ARO = 5), z których każdy oznacza średnio 15 000 € straty na danych i wydajności produkcji (SLE = 15 000). Proponowane rozwiązania zabezpieczające (oprogramowanie antywirusowe) ma zablokować 80% ataków (współczynnik zmniejszenia ryzyka = 80%) i kosztuje 25 000 € rocznie (opłaty licencyjne 15 000 € + 10 000 € za szkolenia, instalację, konserwację itp.). Spodziewany zwrot z inwestycji wynosi zatem:

$$ROSI = \frac{(5 \times 15000) \times 0{,}8 - 25000}{25000} = 140\%$$

Przedstawiona metodyka ma dość ograniczone zastosowanie. Wynika to z konieczności szacowania strat w danym roku, czyli przyjmowania że zdarzenie w danym roku z pewnością nastąpi. Jest to prawdziwe jedynie dla niewielu rodzajów ryzyka. Jednak sam fakt, że istnieją już metody pozwalające opierać inwestycje w bezpieczeństwo na rachunku zysku i strat wskazuje na konieczność włączania do zarządzania ryzykiem elementów ekonomiki.

5.5. Podsumowanie rozdziału

Ryzyko operacyjne, mimo że formalnie nieuwzględniane w przepisach prawa, oddziałuje na sposób realizacji zadań przez struktury powoływane celem zarządzania ryzykiem w ramach administracji publicznej. Dotyczy to zarówno działań minimalizujących ryzyko bezwarunkowe, jak i warunkowe. Ma również odniesienie do wszystkich aspektów działań, tj. zorientowanych na sprawność, zorientowanych procesowo, zorientowanych na logistykę oraz zorientowanych na społeczne zaufanie. Ryzyko operacyjne wiąże się również z kosztami ponoszonymi zarówno na minimalizowanie przyszłych strat podczas podejmowania decyzji w warunkach niepewności, jak i z nakładami na minimalizowanie ryzyka.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Rozdział VI
Zarządzanie ryzykiem wystąpienia sytuacji kryzysowej

Jak już zostało wykazane, ryzyko operacyjne ma wpływ na zarządzanie sytuacją kryzysową związaną z możliwością zmaterializowania się ryzyka warunkowego. W tym przypadku nie mamy możliwości oddziaływania na źródło (przyczynę) ryzyka. Pozostaje jednak możliwość oddziaływania na podatność oraz wielkość potencjalnych skutków. W kolejnym rozdziale oba te kierunki oddziaływania zostały szczegółowo przeanalizowane. Badania z tym związane odnosiły się do tezy nr 6 (w zakresie konieczności jednoczesnego zarządzania ryzykiem warunkowym oraz powiązanym z nim ryzykiem operacyjnym). Były one oparte o podejście procesowe. Zasadniczą metodą było analiza przypadków (*case study*).

6.1. Zarządzanie podatnością

Jak już wcześniej zostało przedstawione, w myśl UZK zarządzanie sytuacją kryzysową obejmuje następujące etapy:

- zapobieganie sytuacjom kryzysowym,
- przygotowanie do przejmowania nad nimi kontroli w drodze zaplanowanych działań,
- reagowanie w przypadku wystąpienia sytuacji kryzysowych,
- usuwanie ich skutków oraz odtwarzanie zasobów i infrastruktury krytycznej.

Jednocześnie biorąc pod uwagę, że zarządzanie sytuacją kryzysową związane jest ze wcześniejszym zmaterializowaniem się ryzyka bezwarunkowego, w tej fazie działania systemu ZK nie ma możliwości zapobiegania czynnikom mogącym wywołać sytuację kryzysową. Dlatego realizacja ww. cyklu polega na wykonywaniu następujących działań:

- zmniejszenie podatności poprzez zbudowanie barier systemowych i suplementowych;
- zaplanowanie, zgromadzenie i utrzymywanie w gotowości niezbędnych zasobów;
- uruchamianie procedur zarządzania kryzysowego przy jednoczesnym utrzymywaniu ciągłości działania;
- odtwarzanie zużytych zasobów.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Ustawa opisuje etap przygotowania do działań (realizacja cyklu planowania cywilnego) i etap reagowania (uruchamianie procedur będące zadaniem poszczególnych CZK). Ponadto zakłada, że odtwarzaniem zasobów zajmuje się każdy z uczestników systemu ZK w ramach realizacji swoich zadań własnych. W ustawie pominięto natomiast istnienie ryzyka operacyjnego, którego zmaterializowanie się może zakłócić planową reakcję na wystąpienie ryzyka warunkowego. Ustawa pomija też możliwość zarządzania ryzykiem wystąpienia sytuacji kryzysowej poprzez zmniejszanie podatności.

Zmniejszanie podatności jest dla systemu ZK nowym zagadnieniem, dlatego problematyka ta wymaga szczegółowego omówienia. Na wstępie należy zauważyć, że proces przechodzenia od niekorzystnego zdarzenia do ujawnienia jego społecznych następstw nie jest procesem jednolitym. Często pierwotne zagrożenie wywołuje efekty domina lub efekty kaskadowe. W rezultacie skutki wtórne mogą być o wiele poważniejsze niż te bezpośrednio związane z czynnikiem, który je spowodował – vide katastrofa w Fukushimie („Risktec Newsletter", Spring 2012). Nie zawsze również właściciel ryzyka bezpośrednio związanego z zagrożeniem jest właścicielem ryzyka oddziałującego na społeczność lokalną. Istnieje również możliwość, że ryzykiem nie można zarządzać.

Wielkością, która ma obrazować cechy środowiska sprzyjające lub zabezpieczające przed spełnieniem się ryzyka, jest podatność (*vulnerability*). Określenie to nie jest jednoznaczne. Można spotkać autorów, którzy podatność traktują jako odwrotność odporności (Geis 2000) lub jako element wrażliwości, który w korelacji ze skutkami i prawdopodobieństwem decyduje o wielkości ryzyka (*Guide to Risk and vulnerability analyses*, 2012). Podejmowane są również próby włączenia podatności jako kolejnego elementu decydującego o wielkości ryzyka (Roberts 2011). W takim ujęciu wzór na ryzyko sumaryczne przedstawia się następująco:

$$R = P\,[H, V(A), M, E]$$

- R – ryzyko związane z oddziaływaniem wielu czynników (gospodarczych, społecznych, kulturowych, politycznych, ekologicznych, naukowo-technicznych).
- H – zagrożenie;
- A – zagrożony obiekt lub dobro;
- V – podatność/odporność obiektu lub dobra;
- M – środki i sposoby reagowania;
- E – środowisko (znane i nieznane czynniki zwiększające lub obniżające poziom ryzyka);
- P – prawdopodobieństwo wystąpienia (w odniesieniu do miejsca i czasu).

Istnieją również opracowania wskazujące, że podatność jest znaczenie szerszym pojęciem, wręcz decydującym o tym, czy proces spełniania się ryzyka zostanie ograniczony, czy wręcz przeciwnie – wysoka podatność sprawi, że zagrożenie zmieni się w katastrofę (McEntire 2005).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Schemat 16. Powiązanie ryzyka, cech środowiskowych i podatności
Źródło: McEntire 2005, p. 266; tłumaczenie własne. Użyte na schemacie określenie „elastyczność" pochodzi z tłumaczenia pojęcia „resilience", które norma PKN ISO Guide 73 określa jako: „zdolność adaptacyjną organizacji w zmiennym środowisku". W rzeczywistości chodzi jednak o zdolność odzyskania stanu pierwotnego[20]

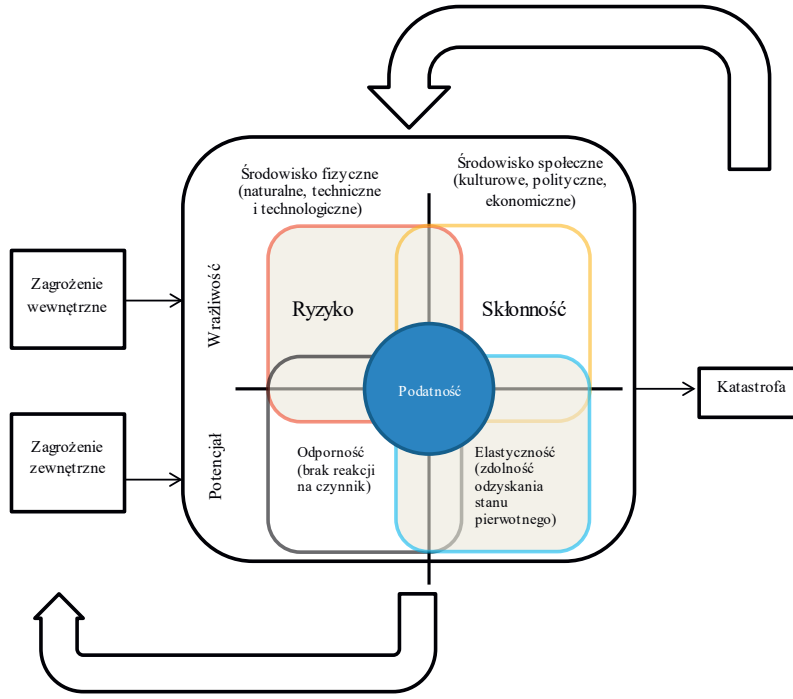
Przedstawione na schemacie zależności należy interpretować następująco. Ryzyko związane z zagrożeniem może dodatkowo się rozprzestrzeniać (lub być ograniczane) ze względu na cechy środowiska, w którym doszło do zdarzenia. Prześledźmy to na przykładzie. Ze względu na stosowaną technologię w zakładzie może dojść do zapłonu. W pewnych warunkach (istnienie atmosfery wybuchowej) zapłon może

[20] Trudności w zrozumieniu przedstawionego schematu wiążą się z użyciem przez autora dwóch różnych pojęć, tj. *resistance* oraz *resilience*. Oba są tłumaczone jako odporność, choć w rzeczywistości ich znaczenie jest różne. Resistance („a force that acts to stop the progress of something or make it slower" – słownik internetowy Cambridge Dictionary) wiąże się z brakiem reakcji na czynnik zakłócający (poprzez wytrzymałość lub opór wobec działającej siły). Resilience („the quality of being able to return quickly to a previous good condition after problems" – słownik internetowy Cambridge Dictionary) wiąże się ze zdolnością do szybkiego odtworzenia stanu wyjściowego (np. poprzez elastyczność lub sprężystość). Zgodnie z definicją przyjętą w tej pracy odporność to „zdolność systemu, społeczności narażonej na zagrożenia do odparcia, wchłonięcia, przystosowania i odbudowy związanej ze skutkami zagrożenia dokonanej w odpowiednim czasie i w skuteczny sposób, włączając w to utrzymanie i odtworzenie ich podstawowych struktur i funkcji [*Risk Assessment and Mapping Guidelines for Disaster Management* 2010]. Ta definicja jest szersza niż stosowana przez autora schematu, gdyż obejmuje dodatkowo adaptację, czyli przygotowanie się i akceptację przyszłej zmiany.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

wywołać wybuch, co oznacza, że istnieje ryzyko powstania zniszczeń spowodowanych tym wybuchem. Jednak czy to ryzyko przekształci się w katastrofę, nie musi być uzależnione wyłącznie od parametrów zdarzenia inicjującego. Elementem decydującym może być podatność środowiska, w którym ryzyko będzie się spełniać. Rozprzestrzeniający się wybuch może napotkać na bariery (np. ściany zbiornika) na tyle odporne, że żadne efekty wtórne nie wystąpią. Jest też możliwym, że w instalacji zastosowano elementy elastyczne (a raczej sprężyste). Takimi elementami mogą być zawory bezpieczeństwa czy uchylne klapy. Wprawdzie nie są one odporne na wzrost ciśnienia, ale po chwilowym odchyleniu mają zdolność powrotu do pozycji prawidłowej. W oby przypadkach środowisko cechuje się małą podatnością, co oznacza, że nie przenosi ryzyka. Istnieje też możliwość, że środowisko jest podatne na dane ryzyko. W tym przypadku rozrywane elementy instalacji mogą doprowadzić do kolejnych awarii i zniszczeń. W efekcie skutki wtórne spowodują, że ryzyko wybuchu w instalacji oznacza ryzyko katastrofy (i związanego z nim kryzysu) dla całego zakładu. To podejście wykazuje zbieżność z koncepcją całościowego rozpatrywania ryzyka w aspekcie ryzyka bezwarunkowego i warunkowego.

W najbardziej skrajnym podejściu podatność jest rozpatrywana niezależnie od ryzyka (ryzyka bezwarunkowego) z uwzględnieniem sprzężeń zwrotnych. Sprzężenia te przedstawiono na schemacie nr 17.



Schemat 17. Powiązanie ryzyka, cech środowiskowych i podatności wraz ze sprzężeniami zwrotnymi

Źródło: McEntire, Crocker 2010, p. 58

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Przedstawione sprzężenia można zinterpretować następująco. Każde przebyte zdarzenie kryzysowe uodparnia mieszkańców na kolejne, podobne sytuacje. Znane są wzorce zachowań, zarówno władze, jak i mieszkańcy dbają o niezbędne środki techniczne, wiadomo gdzie i w jakim trybie można uzyskać dodatkową pomoc. Co ważne, nie występuje element zaskoczenia. Przy tych samych warunkach początkowych (podobne charakter i waga zdarzenia, ci sami mieszkańcy, warunki terenowe itp.) zamiast sytuacji kryzysowej możemy mieć zagrożenie wymagające jedynie rutynowych działań.

Z drugiej strony wysoka podatność może mieć istotny wpływ, a wręcz być rzeczywistą przyczyną katastrofy. Jako przykład można wskazać pożar wieżowca Grenfell Tower w Londynie w dniu 14 czerwca 2017 r. (Wyrozębski 2017). Pożar lodówki w mieszkaniu na 3 piętrze z całą pewnością nie był podstawową przyczyną śmierci ponad 70 osób i zniszczenia konstrukcji 24-kondygnacyjnego wieżowca. Przyczyną tragedii była podatność budynku w postaci palnej izolacji termicznej ścian zewnętrznych. Każde źródło ognia, przy tej podatności, doprowadziłoby do tych samych skutków. W tej sytuacji zarządzanie ryzykiem bez uwzględnienia podatności nie może przynieść oczekiwanych efektów. Źródło nadmiernej podatności nie musi być związane z czynnikami technicznymi i posiadanymi zasobami. Według niektórych badaczy (McEntire, Gilmore 2010) katastrofę będącą następstwem huraganu Katrina, poza niewłaściwym planowaniem przestrzennym, brakiem dochodów z podatków i idącym za tym złym przygotowaniem technicznym, spowodowały błędne decyzje Departamentu Bezpieczeństwa Narodowego (*The Department of Homeland Security*). Dla tego podejścia reprezentatywną jest następująca definicja: „katastrofy są w pewnym sensie przejawem podatności systemu społecznego" (Lewis 1999).

Tylko pozornie przedstawione podejścia do podatności są ze sobą sprzeczne, a przynajmniej rozbieżne. Analizując argumenty przedstawiane przez poszczególnych badaczy, można zauważyć, że znaczenie określenia „podatność" jest mocno powiązane z perspektywą osoby, która próbuje podatność ocenić. Jeżeli oceniający jest właścicielem ryzyka (ryzyka bezwarunkowego), podatność środowiska związana z tym ryzykiem jest jedynie jednym z elementów kontekstu, w jakim ryzyko opisujemy. W tym przypadku podatność możemy uwzględnić przy analizie potencjalnych strat lub w ramach współczynnika wrażliwości obrazującego społeczną reakcję na ryzyko.

Dla osoby zarządzającej ryzykiem warunkowym, która nie zarządza ryzykiem bezwarunkowym (a w szczególnym przypadku może nawet nie wiedzieć o jego istnieniu), zmniejszenie podatności jest jedyną możliwością zminimalizowania przyszłych strat. Zmniejszanie podatności jako element działalności technicznej i organizacyjnej ma oparcie w przepisach (np. omówione wcześniej formy oddziaływania państwa na podmioty gospodarcze), normach i dobrych praktykach. O wiele trudniej zarządzać podatnością w odniesieniu do mieszkańców terenów narażonych na skutki zdarzenia, którego się nie spodziewano. W takim przypadku

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

zamiast zmniejszania podatności wobec znanego zagrożenia, można zastosować zmniejszanie podatności ze względu na cele, jakie chcemy osiągnąć, lub dobra, jakie zamierzamy chronić. W zarządzaniu kryzysowym pomocną w określaniu tych celów jest omówiona już metoda „6 ways to die".

6.2. Budowanie barier systemowych i suplementowych

Metodą na zmniejszenie podatności, a jednocześnie organizacyjne i techniczne przygotowanie się na wystąpienie sytuacji kryzysowej jest zbudowanie służb reagowania przy jednoczesnym przygotowaniu zarówno społeczności lokalnej, infrastruktury, jak i terenu do wystąpienia takiej sytuacji. Działalność ta jest ściśle powiązana z oceną ryzyka. Przykładowo dobór wyposażenia jednostek Państwowej Straży Pożarnej jest oparty o ocenę zagrożeń na obszarze powiatu (DzU z 2014 r. poz. 1793, § 2 ust. 2). Planuje się, że dalszy rozwój Krajowego Systemu Ratowniczo-Gaśniczego będzie oparty głównie na ocenie ryzyka (Wróblewski 2016). Jednak nawet przy najlepiej przygotowanym systemie reagowania mogą wystąpić zdarzenia o takiej skali, że dojdzie do jego niewydolności. Do oceny ryzyka wystąpienia takiej sytuacji stosuje się matrycę ryzyka sytuacji kryzysowej opartą na barierach systemowych i suplementowych (Skomra 2015). Bariery systemowe to bariery ograniczające skutki zagrożeń dynamicznych, tworzące system ochrony społeczności przed zagrożeniami (należą do nich między innymi służby, inspekcje i straże). Bariery suplementowe to bariery ograniczające lub zwiększające skutki zagrożeń dynamicznych, wynikające z wrażliwości i odporności danej społeczności, a mające wpływ na podatność społeczeństwa eksponowanego na zagrożenie. Podatność można zdefiniować jako ekspozycję (wrażliwość) na zagrożenie społeczności w powiązaniu z odpornością. Podatność zawiera dwa elementy: odporność i wrażliwość. Odporność związana jest z panowaniem nad ryzykiem oraz zdolnością redukcji szkód lub poradzenia sobie z nimi. Wrażliwość związana jest z ekspozycją na ryzyko (…). Kombinacja wrażliwości i odporności kreuje podatność na określone zagrożenie (EMA 1999 r., Lewis 2014).

Wrażliwość określa zdolność danej społeczności do poradzenia sobie ze skutkami zdarzenia niekorzystnego, np. zdobyte wcześniej doświadczenie wpływające na zachowanie ludzi w czasie zagrożenia (np. osoby starsze i dzieci są bardziej wrażliwe na dane zagrożenie niż pozostałe osoby itp.). Wrażliwość oceniana jest dla dwóch skutków: „ludzie i „mienie". Ocena polega na oszacowaniu tego, jak mocno wskazana bariera może osłabić działanie barier systemowych w skali od 0 do -10. Gdzie 0 oznacza brak wpływu, zaś -10 – maksymalne osłabienie.

Wrażliwość dla skutków „ludzie" oceniana jest na podstawie barier:

1. Średnia gęstość zaludnienia osób przebywających na stałe w strefie potencjalnego zagrożenia.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

2. Liczba osób przebywających czasowo w strefie potencjalnego zagrożenia.
3. Sezonowy wzrostu populacji.
4. Lokalizacja w strefie zagrożenia szpitali, domów opieki, zamkniętych ośrodków, szkół, przedszkoli, żłobków.
5. Poziom sprawności fizycznej osób w strefie zagrożenia (z uwzględnieniem niepełnosprawnych, dzieci, ludzi w podeszłym wieku, chronicznie chorych).
6. Lokalizacja w strefie zagrożenia obiektów sportowych.
7. Lokalizacja w strefie zagrożenia obiektów handlowych.
8. Inne (szczególnie np. chwilowe zgromadzenia).
9. Lokalizacja w strefie zagrożenia zakładów przemysłowych.

Wrażliwość dla skutków „mienie" oceniana jest na podstawie barier:

1. Obiekty dziedzictwa narodowego, w tym kultu religijnego.
2. Obiekty o dużej wartości.
3. Istnienie obiektów infrastruktury krytycznej.
4. Pola uprawne i sady.
5. Zabudowania.
6. Hodowla i fermy.
7. Szlaki komunikacyjne.

Podatność może wzmacniać bariery systemowe lub osłabiać je. W pierwszym przypadku mamy do czynienia z sytuacją, gdy lokalna społeczność posiada zdolność do radzenia sobie z niebezpieczną sytuacją nawet wówczas, gdy profesjonalne służby ratownicze zawiodą. W drugim przypadku, ze względu na cechy lokalnej społeczności, skutki zagrożenia dynamicznego są większe, niż to wynika z analizy ryzyka pomimo prawidłowej reakcji profesjonalnych służb ratowniczych. Podatność ma więc wpływ na bariery systemowe, a wpływ ten wynika z pojawienia się barier suplementowych.

Budowanie matrycy ryzyka sytuacji kryzysowej polega na obliczeniu wskaźnika gotowości kryzysowej na podstawie oceny wrażliwości i odporności w kategorii „ludzie" oraz w kategorii „mienie". Wartości ryzyka i wskaźnika gotowości kryzysowej decydują o dotkliwości skutków sytuacji kryzysowej, jeśli ona wystąpi. Nanosząc na matrycę obliczony wskaźnik gotowości kryzysowej (oznaczony na schemacie literą „W") oraz poziom ryzyka, uzyskujemy matrycę sytuacji kryzysowej. Wzór takiej matrycy przedstawiono na schemacie nr 18.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

1,0						
0,84						
0,66						
0,5						
0,33						
0,166						
W / Ryzyko	Zaniedbywalne	Małe	Średnie	Duże	Katastrofalne	Ekstremalne

LEGENDA:	
	Zerowa klasa gotowości kryzysowej
	I klasa gotowości kryzysowej
	II klasa gotowości kryzysowej
	III klasa gotowości kryzysowej
	IV klasa gotowości kryzysowej
	V klasa gotowości kryzysowej

Schemat 18. Wzór matrycy ryzyka sytuacji kryzysowej

Źródło: Bralewski A., Piec R., Wróbel R., „Opracowanie wzorcowego scenariusza zagrożenia zgodnie z metodyką zaimplementowaną w narzędziu ARMOR", materiał opracowany w ramach projektu „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP" (projekt nr O ROB/0077/03/003), SGSP 2016 r., s. 28

Uzyskane w ten sposób klasy gotowości kryzysowej oznaczają:

1. Zerowa klasa gotowości kryzysowej – z racji zaniedbywalnej wartości ryzyka zmaterializowania się scenariusza sytuacjom ulokowanym w tej klasie nie poświęca się uwagi (marginalne znaczenie dla rozwoju sytuacji kryzysowej).
2. I klasa gotowości kryzysowej – występująca sytuacja kryzysowa zarządzana jest w sposób rutynowy, jej rozwój jest przewidywalny, małe prawdopodobieństwo kryzysu społecznego, istnieje pewne prawdopodobieństwo, że przekształci się w sytuację kryzysową II klasy.
3. II klasa gotowości kryzysowej – występująca sytuacja kryzysowa wymaga wspomagania zasobami ponadlokalnymi, może wywołać lokalny kryzys społeczno-polityczny. Istnieje prawdopodobieństwo przekształcenia się w III klasę sytuacji kryzysowej.
4. III klasa gotowości kryzysowej – występująca sytuacja kryzysowa wymaga wspomagania centralnego, możliwy kryzys społeczno-polityczny, możliwość wprowadzenia na części terytorium jednego ze stanów nadzwyczajnych, możliwość przekształcenia się w IV klasę gotowości kryzysowej.
5. IV klasa gotowości kryzysowej – występująca sytuacja kryzysowa może wywołać kryzys polityczno-społeczny, a także zagrozić bezpieczeństwu

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

narodowemu, możliwe wprowadzenie jednego ze stanów nadzwyczajnych na terytorium całego kraju.

6. V klasa gotowości kryzysowej – zmaterializowany scenariusz zagrożenia nie został wcześniej uwzględniony w rozważaniach dotyczących szacowania ryzyka występowania zagrożeń. Oznacza to, że zaistniała sytuacja niezależnie od poziomu współczynnika gotowości kryzysowej „W" zawsze spowoduje sytuację kryzysową z uwagi na brak szczegółowych informacji o danym zagrożeniu oraz brak odpowiednich procedur.

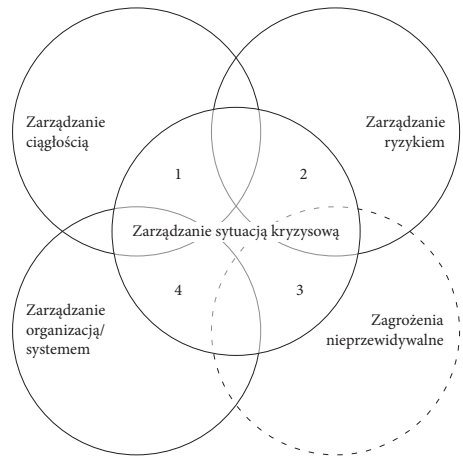
Przedstawiona metodyka pozwala w sposób ekonomicznie uzasadniony podjąć decyzję o skierowaniu (lub nie) środków finansowych w celu obniżenia ryzyka związanego z możliwością wystąpienia sytuacji kryzysowej. Dodatkowo, dzięki sporządzonej ocenie ryzyka, można przewidywać, z jakimi rodzajami sytuacji kryzysowej decydent będzie musiał się zmierzyć.

6.3. Źródła sytuacji kryzysowych

W tradycyjnym ujęciu (Barton 1993) za źródła sytuacji kryzysowych uważa się:

- czynniki losowe (np. powodzie, trzęsienia ziemi);
- problemy techniczne (np. awarie w zakładach produkcyjnych);
- błędy ludzkie (np. katastrofy komunikacyjne);
- błędne decyzje kierownictwa.

Jednak jak wynika z przeprowadzonego procesu badawczego, ryzyko wystąpienia sytuacji kryzysowej jest korelacją ryzyka warunkowego i ryzyka operacyjnego. Tym samym nie można za pomocą prostej listy omówić relacji, jakie zachodzą pomiędzy tymi dwoma rodzajami ryzyka, a których efektem jest ryzyko wystąpienia sytuacji kryzysowej. Na rysunku nr 4 przedstawiono źródła sytuacji kryzysowych z uwzględnieniem tych korelacji.



Rys. 4. Źródła sytuacji kryzysowych

Źródło: opracowanie własne w oparciu o Skomra 2017 b

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Przedstawione na rysunku obszary oznaczone numerami 1–4 odpowiadają następującym zagadnieniom:

1. Ryzyko powstania sytuacji kryzysowej w przypadku gdy zawiedzie zarządzanie ciągłością działania infrastruktury krytycznej, infrastruktury dostarczającej kluczowych usług lub ciągłością funkcjonowania urzędów obsługujących organy administracji publicznej.
2. Ryzyko szczątkowe – ryzyko, którym nie zarządzamy ze względów ekonomicznych (świadomie zgadzamy się, aby w przypadku zmaterializowania się ryzyka doszło do sytuacji kryzysowej).
3. Ryzyko wystąpienia zdarzenia nieprzewidywalnego.
4. Ryzyko wewnątrzsystemowe związane z funkcjonowaniem organizacji lub systemu (np. brak sukcesji władzy w przypadku niedostępności decydenta, zdarzenie, któremu nie przyporządkowano decydenta (UZK używa określenia „organ wiodący"), zdarzenie, któremu przyporządkowano jednocześnie kilku decydentów).

Zagadnienia te zostaną omówione kolejno.

6.3.1. Ciągłość działania

W działalności biznesowej ciągłość działania jest typowym uzupełnieniem zarządzania ryzykiem w przypadku, gdyby działania prewencyjne zawiodły. Ograniczeniem dla wdrażania ciągłości działania są koszty z tym związane. W przypadku gdy wydatki przestają być racjonalne, należy zaprzestać działalności. Z punktu widzenia odbiorcy usługi mającej znaczenie krytyczne takie podejście jest niedopuszczalne. Usługi, których brak oznacza u odbiorcy straty materialne, zagrożenie życia czy zdrowia, powinny być utrzymywane i przywracane po awarii bez względu na koszty. Jednak nawet po odrzuceniu rachunku ekonomicznego jako czynnika powodującego zaniechanie działania istnieje zawsze problem niezawodności technicznej oraz niezawodności systemu organizacyjnego, w wyniku których proces utrzymywania ciągłości działania zawiedzie. Przyczyną zawodności może również być brak wdrożonych rozwiązań w zakresie utrzymania ciągłości działania, co w odniesieniu do urzędów administracji publicznej jest zjawiskiem powszechnym.

Biorąc pod uwagę główny cel zarządzania kryzysowego, którym jest łagodzenie skutków społecznych wystąpienia sytuacji kryzysowej, ciągłość działania należy rozpatrywać w trzech aspektach.:

- ciągłość działania obiektów i systemów zapewniających usługi kluczowe dla społeczeństwa, w tym obiekty IK;
- ciągłość działania urzędów obsługujących organy administracji publicznej (w tym obiekty IK, dla których administracja publiczna jest właścicielem) – ten aspekt jest powiązany m.in. z utrzymaniem sprawności systemu zarządzania kryzysowego, a zatem łączy się z zagadnieniem zagrożeń wewnątrzsystemowych;
- utrzymanie ciągłości zarządzania państwem jako całością.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zagadnienie ryzyka warunkowego będącego następstwem dysfunkcji obiektu IK zostało już omówiona. Jednak zawodność ciągłości działania w każdym z wymienionych obszarów może być źródłem sytuacji kryzysowej, choć nie w każdym przypadku wystąpienie takiej sytuacji jest jej prostym następstwem. Przykładowo po huraganie w lasach tucholskich w dniu 11.08.2017 r. zniszczeniu uległa sieć energetyczna, nie działały telefony stacjonarne (częściowo zniszczone linie napowietrzne, brak awaryjnego źródła energii w urzędach gmin pozwalającego zasilić centrale podłączone do podziemnych linii kablowych) i komórkowe (brak agregatów prądotwórczych zasilających stacje bazowe – tzw. BTS-y). W efekcie, pomimo formalnego obowiązku powiadomienia o zdarzeniu wyższych szczebli administracji publicznej, pozornie poprawnie zaprojektowany obieg informacji w ramach systemu zarządzania kryzysowego okazał się zawodny. Niezbędna reakcja ze szczebla centralnego nastąpiła z co najmniej jednodniowym opóźnieniem. Utrzymanie ciągłości procesów pomimo wystąpienia awarii wiąże się nie tylko ze sprawnością struktur ratowniczych i zarządzania kryzysowego. W niektórych przypadkach może wprost oznaczać zagrożenie dla zdrowia i życia. Przykładowo wdrażany system e-recepta, o ile nie będzie zawierał rozwiązań awaryjnych, może doprowadzić do sytuacji, gdy pacjent nie będzie w stanie zakupić leku ratującego życie.

W najszerszym podejściu konieczność utrzymania ciągłości dotyczy struktur państwa i jest odpowiedzią na zagrożenia hybrydowe i militarne. Zagadnienie to znalazło się w dokumencie „Zobowiązanie do wzmocnienia odporności" (*Commitment to enhance resilience*) będącym jednym z postanowień przyjętych podczas szczytu NATO w Warszawie (Meyer-Minnemann 2016). Zapewnienie ciągłości zarządzania państwem jest, w myśl tego dokumentu, jednym z siedmiu obszarów odporności sojuszu na zagrożenia hybrydowe i militarne. Warto jednocześnie zwrócić uwagę, że należy rozróżniać pojęcia „ciągłość działania rządu" (*Continuity of Government*), która jest kojarzona z działalnością polityczną, od pojęcia „ciągłość rządzenia" (*Continuity of Governance*), która sprowadza się do działań w zakresie tworzenia zasobów i działań organizacyjnych pozwalających na utrzymanie zdolności zarządzania państwem pomimo wystąpienia sytuacji kryzysowej. To drugie podejście naturalnie koresponduje z zarządzaniem ryzykiem operacyjnym (Skomra 2016 b, *Building resilience in response to modern and traditional threats*, prezentacja przedstawiona podczas seminarium „Continuity of Government", Warszawa 21–22.09.2016).

Na zakończenie prowadzonych rozważań należy odnotować, że według obecnego stanu prawnego utrzymanie ciągłości działania dotyczy jedynie jednego z zagadnień wchodzących w obszar zarządzania kryzysowego (Skomra 2016), a wiąże się z utrzymaniem usług realizowanych przez infrastrukturę krytyczną (Pyznar 2010). Dodatkowo uchwałą RM (NPOIK, s. 21) został wprowadzony obowiązek zapewnienia ciągłości działania urzędów obsługujących ministrów odpowiedzialnych za funkcjonowanie poszczególnych systemów IK.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

6.3.2. Zarządzanie ryzykiem bezwarunkowym i warunkowym

Zazwyczaj proces zmniejszania ryzyka nie eliminuje go całkowicie. Ze względów finansowych (zbyt duże nakłady na zmniejszanie ryzyka w stosunku do spodziewanych strat, o ile ryzyko się zmaterializuje) lub technicznych (brak możliwości oddziaływania na ryzyko) pozostaje obszar ryzyka, który wymaga odrębnego traktowania. Ten rodzaj ryzyka nosi nazwę ryzyka rezydentnego (*residual risk*) [SO/ IEC 27001 (PN-ISO/ IEC 27001)]. O ile poziom ryzyka rezydentnego jest nieakceptowalny, należy podjąć działania w celu jego przeniesienia. Taki transfer ryzyka może polegać na przykład na jego współdzieleniu (podwykonawcy przejmują na siebie część ryzyka należącego do głównego wykonawcy) lub na wytransferowaniu do podmiotu zewnętrznego (np. ubezpieczenie).

W przypadku administracji publicznej postępowanie z ryzykiem jest ściśle uzależnione od jego charakteru. W przypadku zagrożeń powodziowych minimalizuje się ryzyko bezwarunkowe (właściwa gospodarka wodna, zmniejszanie podatności poprzez odpowiednie planowania przestrzenne). Zarządza się również ryzykiem warunkowym poprzez przygotowanie zasobów uruchamianych na wypadek, gdy zarządzanie ryzykiem bezwarunkowym okaże się nieskuteczne. Dopiero gdy rozwiązania zawarte w gminnych, powiatowych i wojewódzkim planie przeciwpowodziowym zawiodą, uruchamia się system zarządzania kryzysowego. W przypadku innych zagrożeń nie stosuje się tak rozbudowanych metod redukcji ryzyka. Dla huraganów nie ma możliwości zarządzania ryzykiem bezwarunkowym. Zarządza się jedynie podatnością poprzez odpowiednie wymogi techniczne dla obiektów budowlanych. Nie przewiduje się też specjalnych rozwiązań dla fazy reagowania. Minimalizacją skutków zajmują się służby ratownicze w ramach działań rutynowych, a jeżeli te będą niewystarczające, powstaje sytuacja kryzysowa, którą zarządza system zarządzania kryzysowego. W tym przypadku przejście od zagrożenia do sytuacji uważanej za kryzysową jest o wiele szybsze. Istnieje też grupa zagrożeń, których wystąpienie jest równoznaczne z wystąpieniem sytuacji kryzysowej. Polska nie posiada elektrowni jądrowych ani innych obiektów, których awaria mogłaby spowodować obszarowe skażenia radiacyjne. Dlatego ustawa Prawo atomowe regulująca te zagadnienia (DzU z 2017 r. poz. 576, art. 84) przewiduje tylko trzy przypadki. Zdarzenie lokalne (jego obsługą zajmują się służby zakładowe właściciela źródła promieniotwórczego), zdarzenie zarządzane na szczeblu województwa przez wojewodę oraz zdarzenie krajowe zarządzane przez ministra właściwego do spraw wewnętrznych. Te rozwiązania można podsumować następująco. Administracja publiczna nie jest właścicielem ryzyka bezwarunkowego związanego możliwością wystąpienia obszarowego skażenia radiacyjnego. Nie ma też możliwości zmniejszania podatności na to ryzyko. Zatem każde zdarzenie o większej skali niż incydent w zakładzie posiadającym źródło promieniotwórczej, jest sytuacją kryzysową wymagającą działań na poziomie wojewódzkim lub centralnym. Upraszczając można stwierdzić, że wobec ograniczonych możliwości zarządzania ryzykiem

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

bezwarunkowym lub warunkowym administracja publiczna przenosi to ryzyko na system zarządzania kryzysowego.

6.3.3. Zagrożenia wewnątrzsystemowe

Zakłócenie funkcjonowania systemu zarządzania kryzysowego to nie tylko ograniczony dostęp do zasobów osobowych, materialnych, informacyjnych i finansowych spowodowany wystąpieniem czynników wewnętrznych i zewnętrznych. W przypadku złożonych struktur wielopodmiotowych (a taką strukturą jest system zarządzania kryzysowego) źródłem sytuacji kryzysowej może być również:

- wystąpienie zdarzenia nie przyporządkowanego żadnemu systemowi reagowania;
- kryzys współdziałania różnych systemów reagowania (np. brak koordynacji działań pomiędzy Krajowym Systemem Ratowniczo-Gaśniczym, a jednostkami Sił Zbrojnych RP);
- niewydolność systemu wiodącego (przykładowo służby weterynaryjne nie dysponują żadnymi odwodami na wypadek niewydolności na poziomie powiatowym).

Jedną z przyczyn niewydolności wiodącego systemu reagowania może być jego ograniczony zasięg (brak odwodów, brak koordynacji na niektórych poziomach administracji publicznej). Zasięg wybranych systemów reagowania przedstawiono w tabeli nr 28.

Tabela 28. Zasięg wybranych systemów reagowania

Nazwa systemu	*Poziom lokalny*	*Regionalny*	*Krajowy*
Ratownictwo (KSRG)	X	X	X
Ewakuacja	X	X	
Bezpieczeństwo publiczne (Policja)	X	X	X
Utrzymanie warunków bytowych	X		
Ratownictwo medyczne		X	
Ochrona radiologiczna (służba awaryjna Prezesa PAA)			X

Źródło: opracowanie własne

Analizując możliwe powody zawodności systemu zarządzania w sytuacji kryzysowej (Kitler 2000), należy zwrócić również uwagę na istnienie relacji wewnątrzorganizacyjnych wynikających z faktu, że funkcjonowanie systemu reagowania (organizacji) wymaga współdziałania organu zarządzającego z organami wykonawczymi. Przyjmując dla uproszczenia, że zarządzanie systemem jest jednoosobowe, po uwzględnieniu oddziaływania otoczenia oraz oddziaływań wewnętrznych, aktualny stan systemu przedstawiono na schemacie nr 19.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Użyte przy tym zmienne oznaczają:

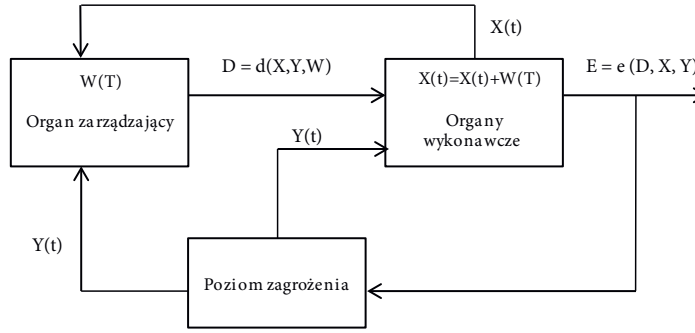
– X – stan wewnętrzny organizacji;

– Y – stan otoczenia (poziom zagrożenia) oddziałujący na daną organizację;

– E – efekt osiągany przez organizację;

– W – stan wiedzy i umiejętności układu zarządzającego.

Przyjmując powyższe założenia, proces zarządzania polega na zebraniu informacji o stanie organizacji (systemu) X (t) i jej otoczenia Y (t), a następnie na przetwarzaniu tych informacji, kierując się wiedzą W (t) organu zarządzającego, w decyzje D (t) realizowane przez organy wykonawcze.



Schemat 19. Uproszczony model procesu zarządzania w sytuacji kryzysowej po uwzględnieniu wektorów stanu organizacji i otoczenia

Źródło: opracowanie własne na podstawie: Kitler 2000, rys. 5, s. 34

Interpretując powyższy schemat, można stwierdzić, że efekt (pozytywny lub negatywny) działań systemu jest uzależniony m.in. od wiedzy decydenta, braku pewności co do posiadania wszelkich informacji niezbędnych do podjęcia decyzji i ryzyka związanego z niepewnością co do efektów skutków podjętej decyzji. Powyższe dylematy związane są z pojęciem ryzyka w teorii podejmowania decyzji (Piśniak 2015). Jeżeli dodamy, że w sytuacjach kryzysowych decyzje podejmowane są pod presją czasu, mediów i oczekiwań osób poszkodowanych, to okaże się, że poprawność funkcjonowania systemu w znacznym stopniu uzależniona jest od wiedzy i intuicji osoby podejmującej decyzje.

6.3.4. Zdarzenia nieprzewidywalne

W zarządzaniu ryzykiem operacyjnym dąży się do pełnej identyfikacji ryzyka. W zarządzaniu kryzysowym świadomość swoich ograniczonych zdolności identyfikacji zagrożenia i oceny związanego z nim ryzyka w połączeniu ze zdolnością do radzenia sobie w razie wystąpienia zdarzenia, „o którym wiem, że nie wiem", świadczy o dojrzałości systemu[21]. Przypadki zdarzeń nieprzewidywalnych (autor

[21] *We plan for the things we know, but we also plan for the things we don't know*, W. Craig Fugate, dyrektor Amerykańskiej Agencji Zarządzania Kryzysowego (*Federal Emergency Management Agency*), „Seminar on Preparing for Extreme Space Weather", Bruksela, 13–15.11.2013.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

używa wobec nich określenia „niespodzianki" – „Surprises"), zostały podzielone na trzy grupy (Michell 1996):

- zdarzenie jedyne w swoim rodzaju, przez co nie można precyzyjnie określić jego skutków (np. dziura ozonowa czy skutki wybuchów na słońcu);
- pierwsze w danym rodzaju, czyli takie, które wystąpiło po raz pierwszy w historii lub występowało, ale nie było kojarzone z zagrożeniem (np. ujawnienie skutków stosowania pestycydu DDT, problem roku 2000, fala ciepła w 2003 r.);
- zdarzenia najgorsze danego rodzaju, czyli pozornie znane, przy czym ryzyko z nim związane zostało niedoszacowane co do prawdopodobieństwa wystąpienia lub jego skutków (np. awaria elektrowni Fukushima).

Do tej listy zdarzeń nieprzewidywalnych należy dodać zagrożenia wynikające z nieujawnionych współzależności. W niniejszym opracowaniu wspominano już o efektach wtórnych, jakie się ujawniły po awarii sieci energetycznej w Szczecinie 2008 r. oraz po pożarze mostu Łazienkowskiego w 2015 r. Równie interesującym przypadkiem, choć nie wywołał większych strat finansowych, jest awaria systemu rowerów miejskich w dniu 11.06.2013 r. jednocześnie w Warszawie, Wrocławiu, Poznaniu i Opolu. Jak się okazało, lokalne spółki zarządzające wypożyczaniem rowerów w ww. miastach korzystały z oprogramowania firmy Nextbike, którego centralny serwer znajdował się w Lipsku. Bezpośrednią przyczyną awarii serwera była powódź, która w tym czasie przechodziła przez Niemcy.

W działalności biznesowej metodą na unikanie zagrożeń wynikających ze współzależności jest zawieranie z dostawcami usług i podwykonawcami umów SLA (*Service Level Agreement*) (NPOIK, zał. nr 1, str. 114). Umowy te powinny określać podstawowe wskaźniki współpracy, terminowość usuwania awarii oraz sankcje za ich nieterminowe usunięcie.

W przypadku systemu zarządzania kryzysowego z góry należy założyć, że nie da się wykryć wszelkich współzależności powodujących przeniesienie awarii z jednego systemu na kolejny, tym bardziej, że część wzajemnie powiązanych systemów jest we władaniu sektora prywatnego, jest zlokalizowana poza terytorium RP lub nie podlega polskiemu systemowi prawnemu. W efekcie administracja powinna planować swoje działania nie tylko wobec zagrożeń znanych, ale również wobec takich, o których nie wie nic lub bardzo niewiele.

Tylko pozornie „spodziewanie się niespodziewanego" jest rozważaniem o charakterze akademickim. Brak zdolności w tym zakresie może mieć skutki wręcz katastrofalne. W ciągu dwudziestu dni sierpnia 2003 r. we Francji na skutek upału zmarło niemal 15 tysięcy osób bez skutecznej reakcji władz (Pirard i in. 2005). Upalne lato spowodowało ponad 70 tysięcy zgonów w całej Europie (Robine i in. 2008]. Próbując wytłumaczyć swoją bezczynność, minister zdrowia Francji Jean-François Mattei podał jako argument nieprzewidywalność zagrożenia oraz fakt, że taka fala upałów dotknęła Francję po raz pierwszy w historii. Stwierdził też, że zdarzenie to nie zostało rozpoznane jako kryzysowe, w efekcie czego nie był

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

on zobowiązany (sic!) do reakcji ani nie posiadał odpowiednich planów reagowania (Jacquat 2003). W jednym z panem ministrem należy się zgodzić. To nie tylko upał był przyczyną tragedii. Złożyły się na nią zmiany demograficzne (starzenie się społeczeństwa) i społeczno-kulturowe (rozpad tradycyjnej formy rodziny, przez co dzieci pozostawiają rodziców bez należytej opieki). Fenomen takich zmian, który wobec bierności władz doprowadza do katastrofy, doczekał się własnych opracowań naukowych (Keller 2015).

Jak pokazuje powyższy przykład, zarządzanie ryzykiem operacyjnym w ramach zarządzania kryzysowego powinno zostać rozszerzone o budowanie zdolności na wypadek zdarzenia nieprzewidywalnego. Dla porządku należy dodać, że zarządzanie sytuacjami nieprzewidywalnymi zostało uwzględnione w brytyjskiej normie BS 11200:2014 *Zarządzanie kryzysowe – wytyczne i dobre praktyki* (*Crisis management – Guidance and good practice*). Jednak ta norma pomija aspekt przygotowywania zasobów i ich uruchamiania w sposób adekwatny do zaistniałego zdarzenia (Abgarowicz 2015).

6.4. Podsumowanie rozdziału

Wystąpienie sytuacji kryzysowej należy wiązać z takimi czynnikami jak:

- zmaterializowanie się bezwarunkowego powodujące wystąpienie zdarzenia krytycznego;
- istnienie ryzyka operacyjnego związanego z rutynowym działaniem administracji publicznej;
- zawodność techniczna systemów i urządzeń dostarczających ludności kluczowych usług;
- podatność środowiska, w którym ryzyko może się rozprzestrzeniać wyrażona przez ograniczoną sprawność barier systemowych i suplementowych;
- możliwość zmaterializowania się ryzyka operacyjnego związanego z działaniem systemu zarządzania kryzysowego.

Swoistym przypadkiem podatności, który to przypadek musi być brany pod uwagę przy pracach planistycznych, jest ograniczona zdolność (lub jej brak) rozpoznania i podjęcia działań minimalizujących skutki zdarzenia, którego nie dało się przewidzieć.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zakończenie

Jednym z zadań administracji publicznej jest zapewnienie bezpieczeństwa. Realizację tego zadania można postrzegać dwojako. Statycznie poprzez stanowienie i egzekucję prawa lub dynamicznie poprzez zarządzanie bezpieczeństwem. Proces zarządzania bezpieczeństwem jest związany z reakcją na spodziewane lub zaistniałe zdarzenie niekorzystne. W przypadku działań długoterminowych związanych z ryzykiem odłożonym, takim działaniem jest odpowiednia polityka państwa. W odniesieniu do zagrożeń występujących w krótszej perspektywie czasowej reakcja na spodziewane zdarzenie to głównie działania prewencyjne polegające na zarządzaniu ryzykiem bezwarunkowym. O skuteczności tego zarządzania decydują głównie czynniki ekonomiczne i ograniczenia techniczne. Świadomość tych ograniczeń jest przesłanką do identyfikowania ryzyka warunkowego oraz zbudowania zasobów (osobowych, materialnych, informacyjnych i finansowych) pozwalających na planową reakcję na wypadek jego wystąpienia. Te zasoby powinny być adekwatne zarówno do wielkości zagrożenia jak i spodziewanych skutków. To oznacza konieczność dokonywania oceny ryzyka, a szerzej zarządzania ryzykiem jako elementu ściśle związanego z zarządzaniem bezpieczeństwem. W fazie reagowania skuteczność działania systemu jest uzależniona od realizacji wcześniej zaplanowanych procesów i to pomimo możliwych zakłóceń. Te zaplanowane procesy muszą uwzględniać również element zaskoczenia i związaną z nim konieczność opanowania nieprzewidzianej wcześniej sytuacji.

Wszystkie te elementy były przedmiotem badań autora, a ich rezultaty pozwoliły na opracowanie niniejszej rozprawy. Ich efekty można sprowadzić do kilku zasadniczych zagadnień przedstawionych kolejno poniżej.

Wnioski ogólne o charakterze teoriotwórczym

Badanie bezpieczeństwa narodowego jest domeną nauk o bezpieczeństwie. Jednak na gruncie tych nauk obszar zarządzania ryzykiem nie został jak dotąd dostatecznie zbadany. Jedną z przyczyn tego stanu rzeczy może być brak odpowiednich narzędzi badawczych. Równolegle badania nad ryzykiem i sposobami postępowania z nim są rozwijane na gruncie nauk o zarządzaniu, w ramach których wypracowano już narzędzia badawcze, podejścia i definicje pojęć. Ta okoliczność została wykorzystana podczas prowadzenia prac badawczych. Ich wyniki można pogrupować w cztery zasadnicze obszary:

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

1. Korzystając z podejścia procesowego, w ramach modelu funkcjonalno-strukturalnego systemu bezpieczeństwa narodowego na poziomie technik i metod można wyodrębnić trzy kategorie ryzyka. Są nimi: ryzyko odłożone, bezwarunkowe i warunkowe. Zastosowany podział ma wymiar praktyczny. Uwzględnia bowiem zarówno formę postępowania z zidentyfikowanym ryzykiem, jak i perspektywę czasową, w jakiej to postępowanie się odbywa. Dodatkowo zaproponowany podział wskazuje na zasadniczy cel podejmowanych działań uwzględniający klasyczny model przyczynowo-skutkowy klasyfikacji ryzyka. W odniesieniu do ryzyka odłożonego są to prowadzone w okresie dłuższym niż 10 lat działania strategiczne związane z prowadzeniem właściwej polityki państwa. W krótszej perspektywie czasowej można natomiast wyodrębnić ryzyka dynamiczne (bezwarunkowe i warunkowe). Dla ryzyka bezwarunkowego perspektywa osiągania celu jest kilkuletnia (ok. 5), zaś działania ukierunkowane są głównie na obniżanie podatności. Dla ryzyka warunkowego (ryzyka wystąpienia sytuacji kryzysowej) perspektywa osiągania celu jest krótka, wynosi 2–3 lata, zaś działania są ukierunkowane na minimalizowanie potencjalnych skutków (szczegóły przedstawiono w rozdziale 3.1). Oba te ryzyka są przedmiotem działań systemu zarządzania kryzysowego (zależności związane z zarządzaniem poszczególnymi rodzajami ryzyka przedstawiono na schemacie nr 8).
2. Elementy składowe systemu zarządzania kryzysowego (zob. tabela nr 13) nie zostały jednoznacznie określone na gruncie prawa. Dlatego w celu opisu systemu należy stosować podejście systemowe w odniesieniu do formalnej struktury organizacyjnej oraz przepływu informacji i zasobów w jej ramach. Równolegle należy wykorzystywać podejście procesowe, co pozwala ujawnić rzeczywiste zależności (procesy) mające wpływ na osiąganie celów (szczegóły przedstawiono w rozdziale 4.2 i 4.3).
3. Bazując na podejściu systemowym, można wykazać, że strukturom zarządzania kryzysowego, nawet tym, które są powoływane tylko doraźnie, przysługuje miano „organizacji" i można im przypisać cele, które powinny osiągać (szczegóły w rozdziale 4.2). Wskazanie celów działania (zob. schemat 11) pozwala wskazać na elementy stanowiące strukturę systemu. W tym również takie elementy, które formalnie sobie nie podlegają, a nawet nie należą do administracji publicznej.
4. Organizacje tworzone na potrzeby zarządzania sytuacją kryzysową, w tym struktury doraźne, aby zarządzać ryzykiem, muszą posiadać niezbędne zasoby materialne, osobowe, informacyjne i finansowe (szczegóły w rozdziale 5.3). Jednocześnie narażone są na oddziaływanie ryzyka operacyjnego (przedstawione na schematach nr 13 i 14). Zarządzanie tym ryzykiem skupia się na problemach związanych z działaniem organizatorskim i dostępnością do zasobów, a jednocześnie wiąże się z zagadnieniem sprawności

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

technicznej oraz utrzymaniem ciągłości działania. Ponadto, jak okazało się w toku badań, oddziaływanie ryzyka operacyjnego należy postrzegać dwojako. Jako możliwość zakłócenia działań administracji publicznej oraz jako możliwość zakłócenia działań systemu zarządzania kryzysowego, który jest elementem ciągłości działania tej administracji. W efekcie można postawić tezę, że definicja ryzyka operacyjnego jest uzależniona od perspektywy, z której oceniamy cele, jakie administracja publiczna zamierza osiągnąć. I tak dla administracji publicznej ryzyko operacyjne jest to ryzyko negatywnego oddziaływania na życie i zdrowie ludzi, mienie (w tym dziedzictwo kulturowe), środowisko naturalne, gospodarkę i infrastrukturę krytyczną oraz ryzyko strat materialnych i reputacyjnych, wynikających z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku procesu zmian w środowisku naturalnym, polityczno-militarnym i społeczno-kulturowym oraz w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych. Natomiast w odniesieniu do zarządzania sytuacją kryzysową ryzyko operacyjne jest to ryzyko strat materialnych i reputacyjnych oraz odpowiedzialności prawnej, wynikających z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w wyniku zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych (Zawiła-Niedźwiecki 2013, s. 62).

Wnioski szczegółowe

1. Wobec administracji publicznej, w tym również wobec tworzonych przez nią struktur doraźnych mających na celu opanowanie sytuacji kryzysowej, uprawnionym jest stosowanie pojęcia „organizacja". Utrzymanie jej działalności pod presją sytuacji kryzysowej wymaga posiadania struktur i zasobów niezbędnych do utrzymania ciągłości działania. Taką strukturą reagowania administracji na wypadek sytuacji kryzysowej jest system zarządzania kryzysowego.
2. W przypadku wystąpienia niekorzystnego zdarzenia skuteczność reakcji administracji związana jest ze sprawnością systemu zarządzania kryzysowego. Ta skuteczność może być ograniczona poprzez zakłócenia wewnętrzne i zewnętrzne wpływające na realizowane procesy.
3. Świadomość, że istnieją takie zakłócenia oraz że ich występowanie jest zjawiskiem typowym w każdej organizacji, jest podstawowym warunkiem poprawy efektywności i wiąże się z zarządzaniem ryzykiem operacyjnym. Istnienie tego ryzyka i konieczność zarządzania nim nie znajduje jak dotychczas odzwierciedlenia w obowiązujących aktach prawnych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

4. Biorąc pod uwagę m.in. postępujące współuzależnienie administracji publicznej i operatorów infrastruktury krytycznej (szczególnie poprzez procesy oparte na wspólnych bazach danych oraz wspólne rozwiązania teleinformatyczne), można postawić tezę, że ilość zakłóceń związanych z infrastrukturą techniczną będzie wzrastała. Jednocześnie sprawność działania struktur administracyjnych, w tym zarządzania kryzysowego, coraz częściej będzie postrzegana z perspektywy niezawodności technicznej.
5. Aby administracja publiczna i operatorzy IK mogli stosować te same zasady ochrony wspólnej infrastruktury, niezbędnym jest rozpowszechnianie podejścia procesowego i opracowanie wspólnych standardów zarządzania ryzykiem operacyjnym związanym z tymi procesami.
6. Zarządzanie ryzykiem operacyjnym realizowane w ramach zarządzania sytuacją kryzysową, poza zidentyfikowanymi zagrożeniami, które są ujęte w procesie zarządzania ryzykiem, musi uwzględniać również zagrożenia nieprzewidywalne. Wiąże się to z zagadnieniem zapanowania nad zdarzeniem, którego rodzaj, skala, sposób oddziaływania lub skutki nie zostały właściwie (w skrajnym przypadku w ogóle) uwzględnione w procesie oceny ryzyka.
7. Czynnikami ryzyka operacyjnego w odniesieniu do zarządzania sytuacją kryzysową są również możliwe zakłócenia procesu decyzyjnego związane działaniem w warunkach niepewności i ryzyka, a jednocześnie pod presją czasu.

Wkład własny autora w rozwój nauk o zarządzaniu

1. Wskazano możliwość wykorzystania osiągnięć nauk o zarządzaniu zarówno w zarządzaniu kryzysowym, jak i w zarządzaniu sytuacją kryzysową realizowanym w ramach administracji publicznej.
2. Powiązano zarządzanie ryzykiem dynamicznym, realizowane w ramach ochrony ludności będącej częścią bezpieczeństwa narodowego, z zarządzaniem kryzysowym i z zarządzaniem sytuacją kryzysową.
3. Ze względu na brak definicji w dostępnej literaturze opracowano definicję zarządzania kryzysowego.
4. Z uwagi na różnice w celach, jakimi kieruje się dana organizacja, rozróżniono obszar zarządzania kryzysowego oraz obszar zarządzania sytuacją kryzysową, gdzie pierwszy obszar zajmuje się planowym zarządzaniem ryzykiem warunkowym, zaś drugi jest formą utrzymania ciągłości działań administracji publicznej na wypadek zmaterializowania się ryzyka warunkowego.
5. Opracowano schemat osiągania gotowości zarządzania ryzykiem, bazując na strukturze funkcjonalnej utrzymywania bezpieczeństwa narodowego oraz wymogach formalnych wynikających z UMOL.
6. Pogrupowano źródła ryzyka sytuacji kryzysowych dla publicznego zarządzania kryzysowego.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

7. Wykorzystując podejście procesowe, wykazano, że zarządzanie sytuacją kryzysową łączy się z zarządzaniem ryzykiem warunkowym wraz z towarzyszącym mu ryzykiem operacyjnym.
8. Bazując na propozycji Komitetu Bazylejskiego opracowano propozycję definicji ryzyka operacyjnego z punktu widzenia celów administracji publicznej.
9. Przedstawiono dualizm postrzegania ryzyka operacyjnego w zależności od tego, czy to ryzyko oddziałuje na cele realizowane w ramach administracji publicznej, czy na cele, którymi kieruje się zarządzanie kryzysowe.
10. Pogrupowano formy zarządzania ryzykiem, jakich administracja publiczna wymaga od własnych jednostek organizacyjnych oraz innych podmiotów, w tym również od podmiotów gospodarczych.
11. Wyjaśniono różnice literaturowe i definicyjne w podejściu do podatności, bazując na podziale ryzyk dynamicznych na bezwarunkowe i warunkowe.

Obszary wymagające dalszych badań

1. Kontynuując badania przedstawione w opracowaniu, należy rozważyć, na ile triada Ryzyko–Bezpieczeństwo–Ciągłość odnosi się do działań administracji publicznej. Pomocnym w tym procesie poznawczym może być cel wdrażania zarządzania ryzykiem w administracji publicznej, czyli budowa odpowiedniego poziomu gotowości w obszarze finansowym, technicznym i organizacyjnym.
2. O ile wymagane przez UMOL osiągnięcie przez administrację gotowości finansowej na wypadek sytuacji kryzysowej powinno być przedmiotem badań w ramach dyscyplin ekonomia i finanse, to osiągnięcie właściwego poziomu gotowości w aspekcie technicznym (zasoby) i organizacyjnym (kadry, struktury) leży w zakresie zainteresowania nauk o zarządzaniu, gdyż są to obszary właściwe dla zarządzania ryzykiem operacyjnym.
3. Wykazany w niniejszym opracowaniu dualizm w postrzeganiu ryzyka operacyjnego wymaga poszerzonych badań z uwzględnieniem współzależności, jakie istnieją w relacjach pomiędzy administracją, operatorami infrastruktury krytycznej oraz zarządzaniem kryzysowym rozumianym jako element utrzymania ciągłości działania.
4. Ryzyko operacyjne związane z zarządzaniem sytuacją kryzysową należy poszerzyć o element związany z możliwymi zakłóceniami związanymi z podejmowaniem decyzji pod presją czasu w warunkach niepewności i ryzyka. To oznacza konieczność przeprowadzenia badań na gruncie teorii decyzji.
5. Dodatkowo należy opracować kryteria pozwalające na dokonanie oceny dojrzałości organów zarządzających sytuacjami kryzysowymi do radzenia sobie z ryzykiem wystąpienia przewidywalnych i nieprzewidywalnych zdarzeń.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Załącznik
– Raport z badań

Badania, których efektem jest niniejsze opracowanie, prowadzone były początkowo na potrzeby procesu doskonalenia systemu zarządzania kryzysowego. Autor, będąc odpowiedzialnym m.in. za bieżącą ocenę poprawności funkcjonowania systemu, miał możliwość wszechstronnego testowania systemu i analizy danych związanych z jego faktycznymi reakcjami. Szczególnie cennym elementem badań była możliwość prowadzenia eksperymentów. Impulsem do poszerzenia badań na zagadnienia związane z oceną ryzyka i zarządzanie ryzykiem było przyjęcie UMOL. Dodatkową inspiracją były efekty dyskusji i prac koncepcyjnych, jakie prowadzono, przy udziale autora w ramach grup roboczych CEPC (m.in. „Join Resilience Seminar" w Oslo 12–13 maja 2016), a w szczególności prace nad wytycznymi w zakresie wzmocnienia odporności w ramach NATO w siedmiu podstawowych obszarach. Są nimi[21]:

1. Zapewnienie ciągłości rządzenia oraz krytycznych usług rządowych.
2. Odporność zaopatrzenia w energię.
3. Zdolność radzenia sobie z niekontrolowanym masowym przemieszczaniem się ludności.
4. Odporność systemu zaopatrzenia w żywność i wodę.
5. Zdolność do radzenia sobie z masową liczbą ofiar.
6. Odporność cywilnych systemów komunikacji.
7. Odporność cywilnych systemów transportu.

Ostatecznie opracowywany dokument został wdrożony w NATO pod nazwą *Resilience Guidelines for Seven Baseline Requirements* (materiał niejawny o klauzuli „do użytku służbowego w ramach NATO").

Posiadana wiedza na temat występowania zakłóceń w działaniu systemu zarządzania kryzysowego oraz zebrane informacje o kierunkach niezbędnych zmian wynikających ze zmieniających się warunków prawnych były podstawą do rozpoczęcia własnych prac nad tymi zagadnieniami.

[21] Zob.: https://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm [dostęp 13.12.2017].

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

1. Faza wstępna (badania *action research* wspierane przez studium przypadku)

Jednym z elementów systemu zarządzania kryzysowego jest proces stałego doskonalenia struktur, planów i obiegu informacji. W ramach tego zadania realizowane są testy procedur i treningi personelu w ramach ćwiczeń pod kryptonimem „Impus". O wiele szerszy zakres mają ćwiczenia z serii „Libero". Te ćwiczenia służą sprawdzeniu reakcji struktur zarządzania kryzysowego na wcześniej określoną sytuację kryzysową. Pomimo że ćwiczący znają założenia ćwiczeń, sam ich przebieg jest sterowany zdarzeniami. Oznacza to, że kolejne wydarzenia pojawiające się w trakcie ćwiczeń (o ich kolejności i zakresie decyduje zespół sterujący) zmuszają ćwiczących do modyfikacji już podjętych decyzji i podejmowania nowych. W efekcie głównym elementem podlegającym ocenie jest proces podejmowania decyzji i powiązany z nim obieg informacji. Istotną częścią ćwiczenia jest komunikowanie kryzysowe polegające na sprawdzeniu możliwości właściwego przekazywania informacji dla ludności (poszczególni rzecznicy prasowi i decydenci muszą przygotowywać i przekazywać właściwe komunikaty w reakcji na zasymulowane informacje telewizyjne i prasowe).

Pierwszymi ćwiczeniami, jakie zostały przeprowadzone w tej formule, były ćwiczenia Libero 2012 mające sprawdzić poziom przygotowań poszczególnych służb do zabezpieczenia przebiegu Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012. Podczas symulowanych wypadków i katastrof ujawniono szereg przypadków niewłaściwego obiegu informacji i zakłóceń w procesie podejmowania decyzji. Po wprowadzeniu korekt w procedurach i schemacie obiegu informacji zarządzono drugą edycję ćwiczenia. W tym przypadku wynik ćwiczeń pozwolił uznać, że stan przygotowań jest zadowalający. Jak się okazało w praktyce, w trakcie turnieju pojawiły się trzy spośród czterech zagrożeń generujących najwyższy poziom ryzyka w myśl dokumentu pt. *Aneks do Krajowego Planu Zarządzania Kryzysowego – Zabezpieczenie Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 w Polsce i na Ukrainie*. Najbardziej dramatycznym zdarzeniem, a zarazem nieprzewidzianym w planach, była konieczność wdrożenia stopnia alarmowego na czas rozgrywania ostatniego meczu na Stadionie Narodowym w Warszawie ze względu na ryzyko ataku terrorystycznego. Było to związane z przejęciem przez Straż Graniczną pakunku zawierającego m.in. materiał wybuchowy oraz mapę okolic stadionu. Analiza typu *case study* przebiegu działań zabezpieczających turniej (w tym wspomnianego zagrożenia o charakterze terrorystycznym) pozwoliła na rozpoczęcie prac nad zmianą zasad planowania fazy reagowania. Uznano, że w miejsce planowania ukierunkowanego na źródło, należy wdrożyć planowania oparte o zestawy zadań (moduły zadaniowe) na tyle elastyczne, by można je było wykorzystać przy każdym, nawet nieprzewidywalnym zdarzeniu.

Analogiczne podejście oparte na eksperymencie zastosowano podczas ćwiczeń Libero 2013, kiedy to zasymulowano pojawienie się w Polsce epizootii afrykańskiego pomoru świń. Wynik eksperymentu był niejednoznaczny. Wprawdzie obieg

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

informacji i decyzji uznano za poprawny, jednak pojawił się czynnik, którego nie przewidywano w planach reagowania. Tym czynnikiem były spodziewane reakcje społeczne związane z podejmowaniem decyzji o sanitarnym uboju świń oraz z zakazami ich hodowli. Plany reagowania na wypadek epizootii nie uwzględniały takich elementów jak odszkodowania związane z zakazem sprzedaży zwierząt czy zapewnienie warunków bytowych rolnikom pozbawionym źródeł utrzymania. Jak się okazało, po faktycznym pojawieniu się ASF w Polsce, początkowe bardzo zdecydowane działania zapobiegawcze zostały znacznie złagodzone ze względu na protesty rolników. Jak wskazuje raport RCB z dnia 8.12.2017 r. w sprawie możliwości wprowadzenia stanu klęski żywiołowej w celu zwalczania epizootii ASF (materiał niepublikowany), pojawił się jeszcze jeden nieprzewidziany wcześniej czynnik, który może być jedną z przyczyn, dla których działania związane z sytuacją kryzysową są nieefektywne[22]. Tym czynnikiem jest skażona żywność przywożona z naruszeniem przepisów przez osoby przyjeżdżające lub wracające z Ukrainy. Jej resztki są wyrzucane do śmieci, którymi żywią się dziki. To może wyjaśniać, dlaczego doszło do przeniesienia choroby z powiatów przy granicy z Białorusią i Ukrainą do miejscowości w okolicach Warszawy. Jednocześnie ten element może sprawić, że wszelkie działania związane z zarządzaniem sytuacją kryzysową okażą się nieskuteczne i z czasem sytuacja kryzysowa przekształci się w kryzys polegający na konieczności zlikwidowania hodowli świń na terenie RP na okres kilku lat, co będzie związane ze stratami finansowymi na poziomie 20 mld zł rocznie oraz z negatywnymi reakcjami rolników pozbawionych środków do życia.

Analogiczną metodę testowania systemu zarządzania kryzysowego poprzez rozgrywanie przez decydentów i uczestników ćwiczenia wcześniej przygotowanych scenariuszy stosuje się w ćwiczeniach z serii CMX (*Crisis Management Exercise*). Są to ćwiczenia struktur NATO ukierunkowane na reagowanie polityczno-militarne w obliczu kryzysu. Określenie „reagowanie kryzysowe" w tym przypadku jest znacznie szersze od tego który jest stosowany przez instytucje cywilne i obejmuje zarówno działania militarne (np. wymuszanie i utrzymywanie pokoju czy działania prowadzone w sytuacjach napięć politycznych poprzedzające obronę kolektywną), jak i niemilitarne (ewakuacje, pomoc ofiarom katastrof i usuwanie skutków katastrof, operacje humanitarne i antyterrorystyczne). Cywilne struktury reagowania kryzysowego są istotnym elementem takich działań, zaś ćwiczenia CMX prowadzone jednocześnie na płaszczyźnie krajowej i międzynarodowej są okazją do wszechstronnego przetestowania obiegu informacji, podejmowania decyzji i poprawności procedur ujętych w poszczególnych planach.

W edycjach ćwiczeń 2015, 2016 i 2017 autor był szefem krajowego zespołu kierowania ćwiczeniem (*Directing Staff*). Zadaniem zespołu kierowania ćwiczeniem był nadzór nad przebiegiem ćwiczenia oraz podgrywanie elementów, których wykonawcy nie zrealizowali, a których brak mógłby zakłócić dalszy tok działań.

[22] W chwili opracowywania niniejszej publikacji działania związane ze zwalczaniem ASF nadal były prowadzone, zaś obszar zagrożony epizootią stale się powiększał.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Jednocześnie zespół kierowania ćwiczeniem dokonywał bieżącej obserwacji, notując swoje spostrzeżenia na odpowiednim formularzu. Po ćwiczeniach każdorazowo dokonywano wstępnej oceny (*Hot Wash-up Discussion*), opracowywano wstępny raport za kraj członkowski (*First Impression Report*), a po całościowym podsumowaniu był opracowywany raport z przebiegu ćwiczenia. Raport łącznie z rekomendacjami był zatwierdzany przez Radę Ministrów.

Wszystkie kroki związane z obserwacją ćwiczeń, notowaniem uwag i opracowywaniem wniosków były realizowane ściśle według zasad obowiązujących w NATO (*Post Excercise Lessons Learned Process 2016*). Szczegóły tego procesu są uściślane na potrzeby danej edycji ćwiczenia i są jednolite dla wszystkich krajów członkowskich. Proces nabywania wiedzy obejmuje trzy następujące po sobie fazy: fazę analizy, której zakończenie oznacza, że zidentyfikowano pewne doświadczenie lub problem, fazę działań naprawczych, po której uznaje się, że ze zidentyfikowanego doświadczenia wyciągnięto wnioski lub wiedzę do stosowania w przyszłości, oraz fazę rozpowszechniania wiedzy. Faza analizy polega na obserwowaniu i dokumentowaniu zagadnień w obszarach: problem, procedura lub dobra praktyka. Następnie poczynione obserwacje poddawane są analizie w zakresie wyjaśnienia przyczyn zjawiska i przygotowania propozycji w zakresie środków zaradczych, które mogą rozwiązać problem oraz w zakresie ciała wykonawczego, które jest władne zaimplementować środki zaradcze. Faza druga (działań naprawczych) obejmuje trzy etapy. Etap wsparcia i określania zadań (decyzje w zakresie udzielania wsparcia przy ustalaniu działań zaradczych, przydział niezbędnych zasobów, określenie zadań dla ciał wykonawczych). Etap implementacji i monitoringu, w którym wykonawca działań przygotowuje plan działań, wdraża go i raportuje postępy (jednocześnie jednostka nadzorująca monitoruje postępy). Ostatni etap w tej fazie to walidacja polegająca na weryfikacji wyników (co oznacza powrót do obserwacji). Po uznaniu, że zebrane doświadczenie zostały wdrożone do działań systemu, następuje faza rozpowszechniania nabytego doświadczenia poprzez udostępnianie, publikacje i promowanie nowych rozwiązań.

Z uwagi na niejawny charakter wszystkich elementów dotyczących ćwiczenia (klauzule od NATO Unclassified do NATO Confidential) nie można w niniejszym opracowaniu przedstawić szczegółowych wniosków z ćwiczeń. Niemniej jednak ponieważ wnioski te są dokumentem rządowym przyjmowanym przez Radę Ministrów, ich efektem są zmiany w obowiązującym prawie oraz w dokumentach planistycznych (plany zarządzania kryzysowego, Plan Reagowania Obronnego RP, plany operacyjnego funkcjonowania poszczególnych urzędów i jednostek organizacyjnych administracji publicznej).

Zarówno ćwiczenia Libero, jak i CMX, a szczególnie eksperymenty przeprowadzane w ich trakcie, wskazały na istnienie czynników ryzyka związanego z funkcjonowaniem struktur zarządzania kryzysowego, które to czynniki nie są uwzględniane w obowiązujących planach i procedurach, a których wystąpienie może zakłócić lub wręcz uniemożliwić osiągnięcie zakładanego celu działania.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Ten etap badań pozwolił na sformułowanie głównego problemu badawczego oraz wstępnych założeń.

2. Faza weryfikacji postawionych tez (badania ilościowe weryfikowane poprzez studium przypadku)

Celem udzielenia odpowiedzi na problemy badawcze, zgodnie z zasadami doboru przypadków do badań (zagadnienie wyłaniania próby badawczej poprzez podział stratygraficzny zostało omówione w rozdziale 1) z zebranej puli przypadków wybrano następujące:

Tabela 29. Tabela podziału stratygraficznego przypadków do badań

Lp.	*Teza/ /Założenie*	*Analizowany przypadek*	*Obszar badawczy/ wynik lub wnioski*
1.	4, 5	Raport sytuacyjny związany z wykryciem w dniu 25.06.2012 r. materiałów wybuchowych w pojemniku na rzece Bug w czasie trwania turnieju EURO 2012.	Reakcja systemu na symptomy zdarzenia, które dopiero może zaistnieć, a które nie zostało uwzględnione w planach.
2.	1, 4	Raport z prac zespołu roboczego RZZK podczas EURO 2012	Działalność doraźnej struktury organizacyjnej o nieznanym wcześniej składzie osobowym i kompetencjach. Efekt synergii. Sformułowano wniosek w sprawie uelastycznienia planowania fazy reagowania (koncepcja modułów zadaniowych).
3.	1, 4	Raport z prac zespołu roboczego RZZK podczas ŚDM 2016	Działalność doraźnej struktury organizacyjnej o nieznanym wcześniej składzie osobowym i kompetencjach. Efekt synergii. Przetestowanie planu reagowania opartego na modułach zadaniowych. Potwierdzenie słuszności przyjętej koncepcji wraz z wnioskiem o zastosowanie tej metody w planach zarządzania kryzysowego na wszystkich szczeblach.
4.	1, 5	Blackout w Szczecinie 8.04.2008 r.	Istnienie współzależności różnych rodzajów infrastruktury pomiędzy sobą pozornie nie powiązanych ze sobą.
5.	3, 4	Pożar mostu Łazienkowskiego w Warszawie 14 lutego 2015 r.	Istnienie współzależności różnych rodzajów infrastruktury pomiędzy sobą, istnienie współzależności administracji publicznej i podmiotów gospodarczych na bazie wspólnych procesów (telekomunikacja, systemy bazodanowe, aplikacje). Wniosek o konieczności wdrożenia zarządzania ciągłością działania w urzędach administracji publicznej.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Lp.	*Teza/ /Założenie*	*Analizowany przypadek*	*Obszar badawczy/ wynik lub wnioski*
6.	1, 2	Wyniki kontroli NIK: „Realizacja przez administrację publiczną województwa podkarpackiego zadań z zakresu infrastruktury przeciwpowodziowej". Nr ewidencyjny P/15/097/ LRZ.	Kompetencje, obowiązki i zadania w zakresie szeroko pojętej ochrony przeciwpowodziowej są znacznie rozproszone pomiędzy różne organy administracji rządowej, samorządowej oraz inne jednostki organizacyjne, co powoduje niską skuteczność i niekompatybilność podejmowanych działań. Wpływ braku elementu koordynacyjnego na sprawność struktury organizacyjnej.
7.	3, 5	Powstawanie COG (centra obsługi gotówki)	Narzucenie zbyt ostrych rygorów prawnych powoduje przenoszenie ryzyka na podmioty zewnętrze, w tym na samą administrację publiczną.
8.	6	Kryzys *Brent Spar*	Brak oceny skutków reakcji społecznej na racjonalną ekonomicznie decyzję powodujący nieprzewidywane straty finansowe.
9.	6	Fałszywa informacja o awarii elektrowni Tihange	Przypadek konieczności zarządzania wzburzeniem społecznym, pomimo że informacja powodująca to wzburzenie była fałszywa.
10.	4, 5, 6	Sprawozdanie z działań podczas huraganu, jaki miał miejsce 11.08.2017 r. w rejonie Chojnic	System zarządzania kryzysowego nie uwzględnia przypadku, gdy podmioty zobowiązane do przekazywania informacji nie są w stanie tego zrealizować (nieuwzględnianie ryzyka operacyjnego w działaniach podmiotów zarządzania kryzysowego). W przypadku rozdźwięku pomiędzy działaniami władz a oczekiwaniami społecznymi pojawia się element samoorganizacji ludności.
11.	2, 3, 4, 5	Awaria elektrowni Fukushima (11 marca 2011 r.)	Efekty wtórne zagrożenia (ryzyko warunkowe) powodujące nieporównywalnie większe straty niż spowodowane przez pierwotną przyczynę zdarzenia (ryzyko bezwarunkowe). Efekt zdarzenia o bardzo niskim prawdopodobieństwie zaistnienia (*Black Swan Event*)
12.	2	Pożar wieżowca Grenfell Tower w Londynie (14 czerwca 2017 r.)	Wpływ podatności na skalę skutków zdarzenia.
13.	2, 6	Katastrofa będącą następstwem huraganu Katrina (29 sierpnia 2005 r.)	Katastrofa spowodowana w równym stopniu skalą zdarzenia (ryzyko bezwarunkowe), co i brakiem właściwego przygotowania (ryzyko warunkowe). Błąd systemu zarządzania kryzysowego spowodowany brakiem formalnego wezwania pomocy ze strony władz lokalnych.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Lp.	*Teza/ /Założenie*	*Analizowany przypadek*	*Obszar badawczy/ wynik lub wnioski*
14.	3, 5	Awaria systemu rowerów miejskich w dniu 11.06.2013 r.	Przypadek istnienia nieujawnionych współzależności systemów.
15.	2, 5	Fala ciepła w Europie 2003 r.	Konieczność uwzględnienia zagrożeń, o których istnieniu nie wiemy aż do momentu pojawienia się skutków. Planowanie reakcji na zdarzenia nieprzewidywalne.

Źródło: opracowanie własne

3. Faza uogólnienia wniosków (badania indukcyjne na bazie *case study*)

Wnioskowanie indukcyjne (od szczegółu do ogółu) pozwala wyprowadzić twierdzenia ogólne na podstawie badania zależności pomiędzy obserwowanymi faktami. Uogólnienie indukcyjne to metoda, która rozszerza przesłankę prawdziwą dla próbki badawczej na całą populację. Jednocześnie jest to wnioskowanie niepełne, co oznacza, że wyprowadzone wnioski są prawdziwe z pewnym prawdopodobieństwem i wymagają dalszych badań potwierdzających lub wykluczających (wspomniana wcześniej zasada łabędzi Poppera). Jak wykazano w rozdziale pierwszym (kontekst badawczy) jest to jednocześnie metoda wystarczająca w przypadku badań teoriotwórczych. Badania prowadzone za pomocą indukcji miały wykazać, że proces zarządzania kryzysowego jest podatny na zakłócenia związane z występowaniem ryzyka operacyjnego. Wynik dociekań wskazuje, że te zakłócenia mają odmienny charakter w odniesieniu do całej administracji oraz w odniesieniu do zarządzania kryzysowego działającego jako jej element zapewniający ciągłość działania. Jednocześnie pojawiają się współzależności pomiędzy administracją, operatorami IK oraz podmiotami tworzącymi system zarządzania kryzysowego, w wyniku których zmaterializowanie się ryzyka w jednym z ww. obszarów oddziałuje (lub może oddziaływać) na pozostałe.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Bibliografia

1. Abgarowicz G. (red.) (2015), *Analiza ryzyka dla zarządzania kryzysowego*, wyd. CNBOP.
2. Abgarowicz G. (red.) (2015), *Pamięć przyszłości. Analiza ryzyka dla zarządzania kryzysowego*, Wydawnictwo CNBOP-PIB, Józefów.
3. Adamiecki K. (1938), *O istocie naukowej organizacji*, Koło Naukowej Organizacji Studentów Politechniki Warszawskiej, Warszawa.
4. Apanowicz J., *Metodologia ogólna*, Wydawnictwo Diecezji Pelplińskiej BERNARDINUM, Gdynia 2002.
5. Auf der Heide E. (1989), *Disaster Response Principles of Preparation and Coordination*, Mosby, St. Louis.
6. Augustyn S. (1998), *Czteroetapowe podejście (zapobieganie, przygotowanie, reagowanie i odbudowa) do klęsk żywiołowych i katastrof technicznych. Zasady planowania i kierowania działaniami w tym zakresie*, AON, Warszawa.
7. Barton R.M. (1993), *Crisis Management*, Oxford.
8. Bennett M., Gupta V. (2010), *Dealing in Security understanding vital services and how they keep you safe.* http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [dostęp: 16.08.2017 r.].
9. „Biuletyn Programu Reformy Administracji Publicznej" nr 15/2001, Instytut Spraw Publicznych, Warszawa.
10. *Black Swan or Blind Spot? The Duality of Extreme Events* (2012), „Risktec Newsletter", Spring 2012.
11. Bochenek M. (2012), *Ryzyko i niepewność w naukach ekonomicznych – rozważania semantyczne*, „Ekonomia Economics" 4(21).
12. Boni M. (red.) (2012), *Państwo 2.0. Nowy start dla e-administracji,* Ministerstwo Administracji i Cyfryzacji, Warszawa.
13. Bonisławska B. (2012), *Współczesne zagrożenia dla bezpieczeństwa publicznego*, „Zeszyty Naukowe WSEI seria: Administracja" nr 1, s. 113–128.
14. Carretta A., Fiordelisi F., Schwizer P. (2017), *Risk Culture in Banking*, Palgrave Macmillan UK.
15. Chlebowski T. (2016), *Obliczanie strat*, „Rządowe Centrum Bezpieczeństwa CIIP Focus" nr 11, listopad 2016.
16. Chung C.J. (2006), *Using likelihood ratio functions for modeling the conditional probability of occurrence of future landslides for risk assessment*, „Computers & Geosciences", Issue 8, pp. 1052–1068.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

17. Ciekanowski Z. (2010), *Rodzaje i źródła zagrożeń bezpieczeństwa. Bezpieczeństwo i technika pożarnicza*, „Bezpieczeństwo i Technika Pożarnicza" nr 1, s. 27–46.
18. Ćwiklicki M., Pawlina A., *Identyfikacja elementów metody „action research" w naukowym zarządzaniu*, „Organizacja i Kierowanie" nr 4/2015 (169), s. 55–69.
19. Ćwiklicki M., *Granice stosowania „action research" w naukach o zarządzaniu*, [w:] *Zarządzanie organizacją z perspektywy metodologicznej. Wybrane zagadnienia*, P. Kuźbik, M. Szymankiewicz (red.), Wyd. UŁ, Łódź 2014, s. 153–162.
20. Czakon W., *Łabędzie Poppera – „case studies" w badaniach nauk o zarządzaniu*, „Przegląd Organizacji" nr 9, 2006, s. 9–13.
21. Darczewska J., *Dezinformacja – rosyjska broń stategiczna*, https://rcb.gov.pl/dezinformacja-rosyjska-bron-strategiczna/.
22. Denuit M., Dhaene J., Goovaerts M., Kaas R. (2005), *Actuarial Theory for Dependent Risks: Measures, Orders and Models*, John Wiley & Sons Ltd, Chichester.
23. DeWolf G.B. (2003), *Process safety management in the pipeline industry: parallels and differences between the pipeline integrity management (IMP) rule of the Office of Pipeline Safety and the PSM/RMP approach for process facilities*, „Journal of Hazardous Materials", Issues 1–3, pp. 169–192.
24. Eisenhower D.D. (1958), *Public papers of the presidents of the United States: Dwight D. Eisenhower 1957,* National Archives and Records Service, Federal Register Division, Washington D.C.
25. *Encyklopedia organizacji i zarządzania*, 1981, PWE, Warszawa.
26. *Enterprise Risk Management – Integrated Framework* (2004), Committee of the Sponsoring Organizations of the Treadway Commission (COSO), New York.
27. Eriksson P., Kovalainen A. (2008), *Qualitative Methods in Business Research*, Sage, London.
28. Fine, W.T. (1971), *Mathematical Evaluation for Controlling Hazards*, „Journal of Safety Research" 3, (4), pp. 157–166.
29. Frańczuk M. (2011), *Zarządzanie ryzykiem w jednostkach sektora finansów publicznych jako jeden ze standardów kontroli zarządczej*, „Finanse, Rynki Finansowe, Ubezpieczenia" nr 42, s. 211–221.
30. Gabryelczyk R. (2006), *ARIS w modelowaniu procesów biznesu*, Difin, Warszawa.
31. Geis, D. (2000), *By design: the disaster-resistant and quality-of-life community*, „Natural Hazards Review", vol. 1, No. 3, pp. 151–60.
32. Gościński J. (1971), *Projektowanie systemów zarządzania*, PWN, Warszawa.
33. Gryz J., Kitler W. (2007), *System reagowania kryzysowego*, Toruń, Wydawnictwo Adam Marszałek.
34. Grzegorczyk W., *Studium przypadku jako metoda badawcza i dydaktyczna w naukach o zarządzaniu*, [w:] *Wybrane problemy zarządzania i finansów. Studia przypadków*, Grzegorczyk W. (red), Wydawnictwo Uniwersytetu Łódzkiego, 2015, s. 9–16.
35. *Guide to Risk and vulnerability analyses* (2012), Swedish Civil Contingencies Agency (MSB).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

36. Hadyniak B. (2010), *Przewidywalność, wartość i ryzyko*, [w:] *Ubezpieczenia. Podręcznik akademicki*, J. Handschke, J. Monkiewicz (red.), Wydawnictwo Poltext, Warszawa.
37. Herman Ch.F. (1963), *Some Consequences of Crisis which Limit the Viability of Organization*, [in:] „Administrative Science Quarterly" No 8/1963, cyt. za Zakrzewska-Bielawska A., *Zarządzanie w kryzysie*, [w:] *Zarządzanie ryzykiem operacyjnym*, Staniec I, Zawiła-Niedźwiecki J.(red.), 2008, Warszawa, Wyd. C.H. Beck.
38. Hood C., Rothstein H., Baldwin R. (2004), *The Government of Risk: Understanding Risk Regulation Regimes*, Oxford University Press, Oxford.
39. *Introdukcja to Return on Security Investment*, European Network and Information Security Agency (ENISA) 2012, www.enisa.europa.eu [dostęp 14.12.2017].
40. Jacquat D. (2003), *Rapport d'information sur la crise sanitaire et sociale déclenchée par la canicule*, tome I, 2ème partie: auditions, Assemblée Nationale, Paris.
41. Jajuga T., Jajuga K., Wrzosek K., Wrzosek S. (1993), *Elementy teorii systemów i analizy systemowej*, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław.
42. Jaworski Z., *Jak to z Czarnobylem było*, „Wiedza i Życie" nr 5/1996.
43. Jedynak P., Szydło S. (1997), *Zarządzanie ryzykiem*, Wydawnictwo Zakład Narodowy im. Ossolińskich, Wrocław–Warszawa–Kraków.
44. Kasznica S. (1946), *Polskie prawo administracyjne. Pojęcie i instytucje zasadnicze*, Księgarnia Akademicka, Poznań.
45. Keller R.S. (2015), *Fatal Isolation. The devastating Paris heat wave of 2003*, The University of Chicago Press.
46. Kitler W. (2000), *Problemy zarządzania kryzysowego w państwie*. Studium, AON, Warszawa.
47. Kitler W. (2011), *Zarządzanie kryzysowe w Polsce, stan obecny i perspektywy*, [w:] *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, Sobolewski G., Majchrzak D. (red.), AON, Warszawa.
48. Knight F.H. (2012), *Risk, Uncertainty and Profit*, Courier Corporation.
49. Kołodziejczyk P., Szołtysek J., *Epistemologia logistyki społecznej*, „Przegląd Organizacji" nr 4, 2009.
50. Kopaliński W. (1989), *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa.
51. Korombel A. (2013), *Apetyt na ryzyko w zarządzaniu przedsiębiorstwami*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa.
52. Kosieradzka A., Zawiła-Niedźwiecki J. (red.) (2016), *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*, edu-Libri, Kraków–Legionowo.
53. Kotarbiński T. (1973), *Traktat o dobrej robocie*, Ossolineum, Wrocław.
54. Koziej S. (2010), *Wstęp do teorii i historii bezpieczeństwa,* skrypt internetowy, Warszawa.
55. Kral Z., Zabłocka-Kluczka A. (2003), *O istocie zjawisk kryzysowych organizacji*, [w:] Skalik J. (red), 2003. *Zachowania organizacji wobec zjawisk kryzysowych*, Wrocław, Cornetis sp. z o.o., s. 20, cyt. za Zakrzewska-Bielawska A., *Zarządzanie w kryzysie*, [w:]

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Zarządzanie ryzykiem operacyjnym, Staniec I., Zawiła-Niedźwiecki J. (red.), Warszawa 2008, Wyd. C.H. Beck.

56. Krukowski K. (2011), *Zarządzanie procesowe w administracji publicznej*, „Współczesne Zarządzanie" nr 1.
57. Krynicka H. (2006), *Koncepcja nowego zarządzania w sektorze publicznym (New Public Management)*, „Studia Lubuskie: Prace Instytutu Prawa i Administracji Państwowej Wyższej Szkoły Zawodowej w Sulechowie" nr 2.
58. Krzyżanowski L. (1994), *Podstawy nauk o organizacji i zarządzaniu*, PWN, Warszawa.
59. Krzyżanowski L. (1999), *O podstawach kierowania organizacjami inaczej*, PWN, Warszawa.
60. *Księga Komunikacji Kryzysowej* (2017), RCB, https://rcb.gov.pl/ksiega-komunikacji-kryzysowej-2017/.
61. Lewis, J. (1999), *Development in Disaster-prone Places*, Intermediate Technology, London.
62. Lisiecki M. (2001), *Klasyczne i nowe metody organizacji i zarządzania*, Wyższa Szkoła Zarządzania i Marketingu w Warszawie, Warszawa.
63. Lorenz Meyer-Minnemann L. (2016), *Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience*, http://transatlanticrelations.org/wp-content/uploads/2016/12/resilience-forward-book-meyer-minnemann-final.pdf.
64. MacDonald C., *Understanding participatory action research: a qualitative research methodology option*, „Canadian Journal of Action Research", volume 13, Issue 2, 2012, pages 34–50.
65. Majchrzak D., *Znaczenie systemu zarządzania kryzysowego w kształtowaniu bezpieczeństwa narodowego*, [w:] *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, Sobolewski G., Majchrzak D. (red.), AON, Warszawa.
66. Marczak J. (2008), *Bezpieczeństwo narodowe – pojęcie, charakter uwarunkowania*, [w:] *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji*, Jakubczak R. (red.), AON, Warszawa.
67. Marszałek M., Sobolewski G., Majchrzak D. (2012), *Zarządzanie kryzysowe w ujęciu narodowym i międzynarodowym*, AON, Warszawa.
68. Matuszak-Flejszman A., Pochyluk R., *Istota kontekstu organizacji w systemowym podejściu do zarządzania*, „Studia Oeconomica Posnaniensia", vol. 4, no. 10, 2016, pp. 9–22.
69. McEntire D.A. (2005), *Why vulnerability matters. Exploring the merit of an inclusive disaster reduction concept*, „Disaster Prevention and Management: An International Journal", vol. 14, Issue: 2, (2005), pp. 206–222.
70. McEntire D.A., Crocker C.G. (2010), *Addressing vulnerability through an integrated approach*, „International Journal of Disaster Resilience in the Built Environment", vol. 1, No. 1, pp. 50–64.
71. Miles M.B., Huberman A.M., Saldaña J. (2014), *Qualitative Data Analysis. A Methods Sourcebook*, Sage Publications, Washington USA.
72. Mitchell J.K. (1996), *The Long Road to Recovery: Community Responses to Industrial Disaster*, United Nations University Press, Tokyo.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

73. Monkiewicz J. (red.) (2004), *Podstawy ubezpieczeń*, Poltext, Warszawa.
74. Nartowski A.S. (2016), *Dobre praktyki spółek notowanych na GPW 2016 – Podręcznik*, Giełda Papierów Wartościowych, Warszawa.
75. Niedbała B., Sierpińska, M. (2003), *Controlling operacyjny w przedsiębiorstwie. Centra odpowiedzialności w teorii i praktyce*, PWN, Warszawa.
76. Nowak E. (2009), *Współczesne poglądy na zarządzanie logistyczne w sytuacjach kryzysowych*, [w:] *Bezpieczeństwo i zarządzanie kryzysowe – aktualne wyzwania. Perspektywy rozwoju teorii i badań nad zarządzaniem bezpieczeństwem*, Włodarczyk M., Marjański A. (red.), „Przedsiębiorczość i Zarządzanie" tom X, zeszyt 5, Społeczna Wyższa Szkoła Przedsiębiorczości i Zarządzania w Łodzi, s. 39–66.
77. Nowak W., Nowak, E. (2009), *Podstawy logistyki w sytuacjach kryzysowych z elementami zarządzania logistycznego*, SWSPiZ, Łódź–Warszawa.
78. Nowosielski S., (2016), *Cele w badaniach naukowych z zakresu zarządzania. Aspekty metodologiczne*, „Prace Naukowe UE we Wrocławiu" nr 421, s. 465–482, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.
79. Nowosielski S., *Cele w badaniach naukowych z zakresu zarządzania. Aspekty metodologiczne*, „Prace Naukowe UE we Wrocławiu" nr 421, s. 468–483.
80. Oniszczuk J. (red.) (2008), *Współczesne państwo w teorii i praktyce. Wybrane elementy*, Oficyna Wydawnicza SGH, Warszawa.
81. Panek B. (2005), *Wybrane problemy współpracy cywilno-wojskowej na poziomie operacyjnym*, Warszawa 2005.
82. Piątek Z. (2008), *Procedury i przedsięwzięcia systemu reagowania kryzysowego*, Warszawa 2008.
83. Pilarczyk A. (2011), *Polityka zarządzania ryzykiem operacyjnym w świetle Rekomendacji M*, „Zarządzanie Publiczne" nr 1, s. 189–201.
84. Pirard P., Vandentorren S., Pascal M., Laaidi K., Le Tertre A., Cassadou S., Ledrans M. (2005), *Summary of the mortality impact assessment of the 2003 heat wave in France*, „Eurosurveillance", vol. 10, No. 7.
85. Piśniak M. (2015), *Ryzyko w teorii podejmowania decyzji*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" nr 19 (2015).
86. Pizło W., *Studium przypadku jako metoda badawcze w naukach ekonomicznych*, „Roczniki Naukowe Stowarzyszenia Ekonomistów Rolnictwa i Agrobiznesu" tom XI, zeszyt 5, Warszawa 2009.
87. Podolski A. (2010), *Miejsce Rządowego Centrum Bezpieczeństwa w systemie bezpieczeństwa antyterrorystycznego Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 2 (2010).
88. Podolski A. (2010), *Przedmowa do monografii*, [w:] *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, W. Skomra (2010b), Presscom, Wrocław.
89. Popper K. (1959), *The logic of scientific discovery*, Hutchinson & Co. Londyn.
90. Power M. (2004), *The Risk Management of Everything. Rethinking the politics of uncertainty*, DEMOS, https://www.demos.co.uk/files/riskmanagementofeverything.pdf.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

91. Pszczołowski T., (1978), *Mała encyklopedia prakseologii i teorii organizacji*, Zakład Narodowy im. Ossolińskich, Wydawnictwo, Wrocław 1978.
92. Pszczołowski T. (1982a), *Dylematy sprawnego działania*, Wiedza Powszechna, Warszawa.
93. Pszczołowski T. (1982b), *Zasady sprawnego działania. Wstęp do prakseologii*, Wiedza Powszechna, Warszawa.
94. Pyznar M. (2010), *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa*, [w:] *Ochrona infrastruktury krytycznej*, Tyburska A. (red.), Wydawnictwo WSPol, Szczytno, s. 103–114.
95. Pyznar M., Abgarowicz G. (2014), *Rola infrastruktury krytycznej w funkcjonowaniu państwa*, [w:] *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, Świątkowska J. (red.), Instytut Kościuszki, Kraków, s. 11–26.
96. Pyznar M. (2017), *Zmiany w systemie ochrony IK*. Prezentacja przedstawiona w trakcie V Ogólnokrajowego Forum Infrastruktury Krytycznej, RCB Warszawa 11.12.2017.
97. *Realizacja przez administrację publiczną województwa podkarpackiego zadań z zakresu infrastruktury przeciwpowodziowej,* informacja o wynikach kontroli NIK, https://www.nik.gov.pl/kontrole/P/15/097/LRZ/ [dostęp: 7.11.2017].
98. Riche J., Lewis J., (2003), *Qualitative Research Practice A Guide for Social Science Students and Researchers*, Sage Publications Ltd, London.
99. Roberts S. (2011), *Covering the Full Spectrum of Risks: Implications for Civil Emergency Planning*. Prezentacja wygłoszona w czasie spotkania Grupy Planowania Cywilnego (NATO CPG) 5.10.2011 r.
100. Robine J.M., Cheung S.L.K., Le Roi S., Van Oyen H., Griffiths C., Michel J.P., Herrmann F.R. (2008), *Death toll exceeded 70,000 in Europe during the summer of 2003*, „Comptes Rendus Biologies", vol. 331, No. 2, pp. 171–178.
101. Ronka-Chmielowiec W. (2010), *Wykorzystanie ubezpieczeń do zarządzania ryzykiem operacyjnym w przedsiębiorstwie*, [w:] *Zarządzanie ryzykiem działalności organizacji*, Monkiewicz J., Gąsiorkiewicz L. (red.), C.H. Beck, Warszawa, s. 47–61.
102. Schneider S.K. (1995), *Flirting with disaster. Public management in crisis situation*, M.E. Shape New York.
103. Schultz M., Hatch M.J. and Larsen H.J. (eds) (2000), *The Expressive Organization: linking identity, reputation and the corporate brand*, Oxford University Press.
104. Shakir, M. (2002), *The selection of case studies: strategies and their applications to IS implementation case studies*, „Research Letters in the Information and Mathematical Sciences" 3, pp. 69–77.
105. Sienkiewicz P. (1994), *Analiza systemowa, metodologia modelowania systemowego*, AON, Warszawa.
106. Skomra W. (red.) (2015), *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego Rzeczypospolitej Polskiej*, SGSP, Warszawa.
107. Skomra W. (2004), *Problemy organizacyjno-prawne współdziałania administracji, wojska i służb ratowniczych w czasie klęski żywiołowej*, „Zeszyty Naukowe AON" nr 1, s. 186–196.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

108. Skomra W. (2005), *Model funkcjonowania organów administracji publicznej w czasie klęsk żywiołowych na obszarze województwa, rozprawa doktorska*, AON, Warszawa.

109. Skomra W. (2010), *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, [w:] *Ochrona infrastruktury krytycznej*, Tyburska A. (red.), Wydawnictwo WSPol, Szczytno, s. 209–219.

110. Skomra W. (2010 b), *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Presscom Wrocław.

111. Skomra W. (2016), *Zarządzanie kryzysowe – praktyczny przewodnik*, Presscom, Wrocław.

112. Skomra W. (2017 a), *Współpraca administracji z sektorem gospodarczym na rzecz ochrony infrastruktury krytycznej*, „Management Science Review" 1(1), 2017, UE Wrocław.

113. Skomra W. (2017 b), *Zarządzanie ryzykiem operacyjnym w administracji publicznej*, „Przegląd Organizacji" nr 7/2017.

114. Skomra W. (2016 b), *Building resilience in response to modern and traditional threats*, prezentacja przedstawiona podczas seminarium „Continuity of Government", Warszawa 21–22.09.2016.

115. Skomra W. (2017 c), *Risk management as part of crisis management tasks*, „Foundations of Management" vol. 9, 2017, pp. 245–256.

116. Skomra W. (2017 d), *Miejsce, rola i zadania Rządowego Centrum Bezpieczeństwa w zakresie integracji działań na rzecz utrzymania bezpieczeństwa*, [w:] *Ratownictwo wodne oraz inne aspekty bezpieczeństwa na obszarach wodnych*, J. Telak (red.), CSP Legionowo.

117. Staniec I., Zawiła-Niedźwiecki J. (2015), *Ryzyko operacyjne w naukach o zarządzaniu*, C.H. Beck, Warszawa.

118. Stec M. (1999), *Zarządzanie w sytuacjach kryzysowych – organy, kompetencje, finanse*, [w:] *Państwo–Rząd–Administracja*, „Biuletyn Programu Reformy Administracji Publicznej ISP" nr 12, wrzesień 1999.

119. Stec M., Płoskonka J., Prutis S. (1999), *System zarządzania państwem w sytuacjach kryzysowych*. Raport Programu Reformy Administracji Publicznej, Instytut Spraw Publicznych, Warszawa.

120. Stoner J.A., Wankel C. (1992), *Kierowanie*, PWE, Warszawa.

121. Stoner J.A.F., Freeman R.E., Gilbert Jr. D.R. (2001), *Kierowanie*, PWE, Warszawa 2001.

122. Szlachcic B. (2014), *Analiza ryzyka i zarządzania ryzykiem jako element systemu zarządzania kryzysowego w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach" nr 103.

123. Szołtysek J. (2014), *Przesłanki i założenia koncepcji logistyki społecznej*, „Gospodarka Materiałowa i Logistyka" nr 2, s. 2–7.

124. Szołtysek J., Twaróg S., (2013), *Koncepcja logistyki społecznej na tle paradygmatu logistyki*, „Studia Ekonomiczne/Uniwersytet Ekonomiczny w Katowicach" nr 175, *Demograficzne uwarunkowania logistyki społecznej*, s. 13–31.

125. Szumowski W. (2009), *Zastosowanie podejścia procesowego w urzędach administracji samorządowej*, [w:] *Podejście procesowe w organizacjach*, Nowosielski S. (red.), „Prace

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" nr 52, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław, s. 106–118.

126. Szymonik A., Bielecki M. (2015), *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*, Difin, Warszawa.
127. Tabasz W. (1999), *Prawne, ekonomiczne i polityczne determinanty funkcjonowania zrzeszeń*, [w:] *Straż ogniowa w środowisku lokalnym*, Tabasz W., Chrobak T. (red.), materiały z konferencji naukowej i podsumowania VI Ogólnopolskiego Konkursu Kronik i VI Konkursu na pamiętniki, wspomnienia, opracowania i relacje „Z dziejów Ochotniczych Straży Pożarnych", Wyższa Szkoła Społeczno-Gospodarcza, Tyczyn.
128. *The NATO Lessons Learned Handbook – Third Edition*, NATO Joint Analysis and Lessons Learned Centre, 2016.
129. Turski W.M. (2013), *Na marginesie*, edu-Libri, Kraków–Warszawa.
130. Waters D. (2001), *Zarządzanie operacyjne. Towary i usługi*, PWN, Warszawa.
131. Willetta A.H. (2002), *The Economic Theory of Risk and Insurance*, University Press of the Pacific.
132. Wodecka-Hyjek A. (2010), *Metodyka Prince 2 w zarządzaniu realizacją projektów*, „Acta Universitatis Lodziensis. Folia Oeconomica" nr 234, s. 361–375.
133. Wójcik P., *Znaczenie studium przypadku jako metody badawczej w naukach o zarządzaniu*, „E-mentor" nr 1(48)/2013.
134. Wojnowski M. (2014), *Terroryzm w służbie geopolityki. Konflikt rosyjsko-ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji „wojny buntowniczej" Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 11 (6), s. 58–90.
135. Wojnowski M. (2015), *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" nr 12 (7), s. 11–36.
136. Wolanin J. (2005), *Zarys teorii bezpieczeństwa obywateli: ochrona ludności na czas pokoju*, Fundacja Edukacja i Technika Ratownictwa, Warszawa.
137. Wróblewski D. (2007), *Komunikacja kryzysowa jako instrument kształtowania bezpieczeństwa*, Warszawa 2007.
138. Wróblewski D. (red.) (2015), *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, Wydawnictwo CNBOP.
139. Wróblewski R. (1996), *Zarys teorii kryzysu, zagadnienia prewencji i zarządzania kryzysowego*, AON, Warszawa.
140. Wrzosek S. (2008), *System: administracja publiczna. Systemowe determinanty nauki administracji*, Wydawnictwo KUL, Lublin.
141. Wyrozębski M., *Płonąca pułapka*, „Przegląd Pożarniczy" nr 8/2017, s. 10–13.
142. Yin R.K., *Case Study Research Design and Methods*, Second Edition, Sage Publ., Londyn 1994.
143. Zapłata, S., Kaźmierczak, M. (2011), *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Oficyna Wolters Kluwer Business, Warszawa.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

144. Zawiła-Niedźwiecki J., Byczkowski M. (2003), *Total Information Security Management -Business Continuity Planning*, European Network Security Institute, Warszawa.

145. Zawiła-Niedźwiecki J. (2013), *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, edu-Libri, Kraków–Warszawa.

146. Zawiła-Niedźwiecki J. (2015), *Ryzyko operacyjne z perspektywy logistyki społecznej*, „Logistyka" nr 4, s. 8606–8613.

147. Zawiła-Niedźwiecki J., Gołąb P. (2010), *Zapewnienie ciągłości działania jako ograniczenie ryzyka operacyjnego*, [w:] *Zarządzanie ryzykiem działalności organizacji*, Monkiewicz J., Gąsiorkiewicz L. (red.), C.H. Beck, Warszawa, s. 187–218.

148. Zieleniewski J. (1975), *Organizacja i zarządzanie*, wyd. IV, PWN, Warszawa.

149. Ziembiński Z., *Logika praktyczna*, Wyd. PWN, 2017.

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Akty prawne i normatywne

1. Aneks do Krajowego Planu Zarządzania Kryzysowego 2012: Zabezpieczenie Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 w Polsce i na Ukrainie, 8 czerwca–1 lipca 2012 roku (2012), RCB.
2. AS/NZS 4360 *Risk management – Standards Australia and Standards New Zealand*.
3. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, https://www.bbn.gov.pl/pl/prace-biura/publikacje/6815, Biala-Ksiega-Bezpieczenstwa-Narodowego-RP.pdf [dostęp: 11.09.2017].
4. Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (DzUrz UE L 347/924).
5. Decyzja Rady nr UE 2007/124/JHA z dnia 12 lutego 2007 r. w sprawie szczegółowego programu „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa" (DzUrz UE L 58).
6. Decyzja Ramowa Rady nr 2002/475/WSiSWz dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu.
7. Dekret z dnia 23 kwietnia 1953 r. o świadczeniach w celu zwalczania klęsk żywiołowych (DzU nr 23, poz. 93 ze zm.).
8. Dyrektywa 2004/108/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 2004 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej oraz uchylająca dyrektywę 89/336/EWG (DzUrz UE L 390/24).
9. Dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim, (DzUrz UE L 288/27).
10. Dyrektywa 2014/30/UE Parlamentu Europejskiego i Rady z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej (DzUrz UE L 96/79).
11. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (DzUrz UE L 194/1).
12. Dyrektywa Parlamentu Europejskiego i Rady 2008/50/WE z dnia 21 maja 2008 r. w sprawie jakości powietrza i czystszego powietrza dla Europy (CAFE) (DzUrz UE L 152 z 11.06.2008).
13. Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (DzUrz UE L 345/75).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

14. Hyogo Framework for Action 2005–2015: *Building the Resilience of Nations and Communities to Disaster*, [in:] *Report of the World Conference on Disaster Reduction*, Kobe, Hyogo, Japan, 18–22 January 2005, A/CONF.206/6, pp. 6–28.
15. Informacja o wynikach kontroli „Ochrona przeciwpowodziowa w województwie małopolskim i świętokrzyskim", nr ew. 179/2009/P09143/LKR, www.nik.gov.pl/plik/id,1408,vp,1447.pdf [dostęp: 11.09.2017].
16. Konstytucja RP (DzU z 1997 r. nr 78, poz. 483 ze zm.).
17. Konwencja Wiedeńska z dnia 24 kwietnia 1963 r. o stosunkach konsularnych (DzU z 1982 r. nr 13, poz. 98).
18. Krajowy Plan Zarządzania Kryzysowego 2013/2015 (2013), RCB.
19. MC 334/1 NATO Principles and Policies for HNS Planning.
20. Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) przyjęty uchwałą nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r., http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf [online 11.09.2017].
21. Norma SO/IEC 27001 (PN-ISO/IEC 27001) *Systemy zarządzania bezpieczeństwem informacji. Wymagania*.
22. *Ocena ryzyka na potrzeby zarządzania kryzysowego – Raport o zagrożeniach bezpieczeństwa narodowego*, RCB 2013, http://rcb.gov.pl/wp-content/uploads/ocenaryzyka.pdf [dostęp: 11.09.2017].
23. Plan zarządzania kryzysowego województwa wielkopolskiego z 2011 r.
24. Policy Guidelines NCRS C – M (2001) 63.
25. *Risk Assessment and Mapping Guidelines for Disaster Management*, Comission Staff Working Paper, SEC (2010) 1626 final, Brussels.
26. *Risk Assessment and Mapping Guidelines for Disaster Management*, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2017833%202010%20INIT [dostęp: 11.09.2017].
27. Rozporządzenie Ministra Finansów z dnia 28 listopada 2008 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące oraz warunków ich stosowania (DzU nr 212, poz. 1338).
28. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (tekst jedn. DzU z 2003 r. nr 169, poz. 1650 ze zm.).
29. Rozporządzenie Ministra Rolnictwa i Rozwoju Wsi z dnia 26 maja 2004 r. w sprawie zakresu i warunków współpracy organów administracji rządowej i jednostek samorządu terytorialnego oraz innych podmiotów w tworzeniu planów gotowości zwalczania chorób zakaźnych zwierząt (DzU poz. 129, poz. 1372).
30. Rozporządzenie Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (DzU poz. 637).
31. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego (DzU nr 46, poz. 239).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

32. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne (tekst jedn. DzU z 2016 r. poz. 793).
33. Rozporządzenie Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa (tekst jedn. DzU z 2015 r. poz. 508).
34. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r., w sprawie wymagań bezpieczeństwa teleinformatycznego (DzU nr 159, poz. 948).
35. Rozporządzenie Rady Ministrów z dnia 15 czerwca 2004 r. w sprawie warunków i trybu planowania i finansowania zadań wykonywanych w ramach przygotowań obronnych państwa przez organy administracji rządowej i organy samorządu terytorialnego (DzU nr 152, poz. 1599).
36. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. DzU z 2016 r. poz. 113).
37. Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które utworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania (DzU nr 226, poz. 1810).
38. Rozporządzenie Rady Ministrów z dnia 17 grudnia 2002 r. w sprawie stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych (DzU nr 239, poz. 2030).
39. Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego (DzU nr 20, poz. 169 ze zm.).
40. Rozporządzenie Rady Ministrów z dnia 20 listopada 2015 r. w sprawie utworzenia Ministerstwa Spraw Wewnętrznych i Administracji (DzU poz. 1946).
41. Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad udziału pododdziałów i oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu (DzU nr 41, poz. 347).
42. Rozporządzenie Rady Ministrów z dnia 21 września 2004 r. w sprawie gotowości obronnej państwa (DzU nr 219, poz. 2218).
43. Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (DzU nr 116, poz. 1090).
44. Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin (DzU nr 96, poz. 50).
45. Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym (DzU nr 98, poz. 978).
46. Rozporządzenie Rady Ministrów z dnia 28 września 1993 r. w sprawie powszechnej samoobrony ludności (DzU nr 91, poz. 421).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

47. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (DzU nr 83, poz. 542).
48. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (DzU nr 83, poz. 540).
49. Rozporządzenie Rady Ministrów z dnia 4 lipca 1992 r. w sprawie zakresu i trybu korzystania z praw przez kierującego działaniem ratowniczym (DzU nr 54, poz. 259).
50. Rozporządzenie Rady Ministrów z dnia 6 sierpnia 2013 r. w sprawie szczegółowych warunków i sposobu użycia oddziałów i pododdziałów Policji oraz Sił Zbrojnych Rzeczypospolitej Polskiej w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego (DzU poz. 1037).
51. Rozporządzenie Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i właściwości organów w tych sprawach (DzU poz. 96).
52. Rozporządzenie Rady Ministrów z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach (DzU poz. 96).
53. *Sendai Framework for Disaster Risk Reduction 2015–2030*, [in:] *Proceedings of the Third UN World Conference on Disaster Risk Reduction*, 14–18 March 2015, Sendai, Japan, UNISDR/GE/2015 – ICLUX EN5000, pp. 13–34.
54. Standard BS 11200:2014 – Crisis management - Guidance and good practice.
55. Uchwała nr 167 Rady Ministrów z dnia 15 września 2015 w sprawie przyjęcia Raportu o Zagrożeniach Bezpieczeństwa Narodowego.
56. Uchwała Nr 8/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach (DzUrz KNF z 2013 r. poz. 6).
57. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107–56, OCT. 26, 2001.
58. USA Patriot Act (P.L. 107–56), Section 1016,: https://cdt.org/files/security/usapatriot/titlex.pdf [dostęp: 22.10.2015].
59. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. DzU z 2013 r. poz. 1166 ze zm.).
60. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (DzU poz. 904).
61. Ustawa z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (tekst jedn. DzU z 2014 r. poz. 1539 ze zm.).
62. Ustawa z dnia 12 grudnia 2013 o cudzoziemcach (DzU poz. 1650, ze zm.).
63. Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (tekst jedn. DzU z 2015 r. poz. 163 ze zm.).
64. Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (tekst jedn. DzU z 2016 r. poz. 23).
65. Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (DzU z 2006 r. nr 122, poz. 851 ze zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

66. Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (tekst jedn. DzU z 2017 r. poz. 1201).
67. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (tekst jedn. DzU z 2014 r. poz. 333).
68. Ustawa z dnia 18 lipca 2001 r. Prawo wodne (tekst jedn. DzU z 2017 r. poz. 1121).
69. Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (DzU nr 65, poz. 404).
70. Ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (DzU nr 62, poz. 504).
71. Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (tekst jedn. DzU z 2015 r. poz. 827 ze zm.).
72. Ustawa z dnia 21 maja 1999 r. o broni i amunicji (DzU nr 53, poz. 549).
73. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (tekst jedn. DzU z 2016 r. poz. 1432).
74. Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tekst jedn. DzU z 2015 r. poz. 525).
75. Ustawa z dnia 24 czerwca 2010 r. o szczególnych rozwiązaniach związanych z usuwaniem skutków powodzi z 2010 r. (DzU nr 123, poz. 835 ze zm.).
76. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. DzU z 2010 r. nr 29, poz. 154 ze zm).
77. Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (tekst jedn. DzU z 2017 r. poz. 736).
78. Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (tekst jedn. DzU z 2017 r. poz. 1204).
79. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. DzU z 2017 r. poz. 209).
80. Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (tekst jedn. DzU z 2013 r. poz. 1232).
81. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jedn. DzU z 2013 r. poz. 885 ze zm.).
82. Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (tekst jedn. DzU z 2016 poz. 1636).
83. Ustawa z dnia 29 listopada 2000 r. Prawo atomowe (tekst jedn. DzU z 2017 r. poz. 576).
84. Ustawa z dnia 29 sierpnia 2002r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (DzU nr 156, poz. 1301 ze zm.).
85. Ustawa z dnia 29 stycznia 2004 r. o Inspekcji Weterynaryjnej (DzU z 2007 r. nr 121, poz. 842).
86. Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (DzU nr 130, poz. 1112 ze zm.).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

87. Ustawa z dnia 30 sierpnia 2002 r. o systemie oceny zgodności (tekst jedn. DzU z 2017 r. poz. 1226).
88. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tekst jedn. DzU z 2013 r. poz. 595 ze zm.).
89. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tekst jedn. DzU z 2016 r. poz. 814).
90. Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (tekst jedn. DzU z 2013 r. poz. 596 ze zm.).
91. Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (tekst jedn. DzU z 2016 r. poz. 1866).
92. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jedn. DzU z 2016 r. poz. 1167 ze zm.).
93. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (DzU nr 88, poz. 553 ze zm.).
94. Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jedn. DzU z 2015 r. poz. 355 ze zm.).
95. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jedn. DzU z 2013 r. poz. 594 ze zm.).
96. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jedn. DzU z 2016 r. poz. 446).
97. Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów (tekst jedn. DzU z 2012 r. poz. 392 ze zm.).
98. Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (tekst jedn. DzU z 2013 r. poz. 757 ze zm.).
99. Wskazówki do przygotowania (aktualizacji) planów zarządzania kryzysowego ministrów i kierowników urzędów centralnych, RCB Warszawa 2012 – materiał niepublikowany.
100. *Zarządzanie ryzykiem – Zasady i wytyczne*, PN-ISO 31000:2012.
101. Zarządzenie nr 67 Prezesa Rady Ministrów z dnia 15 października 2014 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego (MP poz. 926).
102. Zarządzenie nr 67 Prezesa Rady Ministrów z dnia 15 października 2014 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego, (MP poz. 926).
103. Zawiadomienie Komisji – Wytyczne oceny zdolności zarządzania ryzykiem (DzUrz UE 2015/C 261/03).

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z dnia 21 kwietnia 2009 r. (sygn. akt K 50/07, DzU nr 65, poz. 553).

Wyrok Trybunału Konstytucyjnego z dnia 3 lipca 2012 r. (sygn. akt K 22/09, DzU poz. 799).

Wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z dnia 9 stycznia 2013 r. Tytuł: *Przesłanki wydania zarządzenia wójta o ewakuacji z obszarów bezpośrednio zagrożonych* (sygn. akt III SA/Wr 504/12).

Strony internetowe

1. Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, http://www.spbn.gov.pl/ftp/dokumenty/Biala_Ksiega_inter_mm.pdf [dostęp: 16.08.2017].
2. Główny Urząd Statystyczny – portal informacyjny, http://stat.gov.pl/cps/rde/xbcr/bialystok/ASSETS_2006_zmiany_strukturalne_7_slownik_pojec.pdf [dostęp: 12.08.2015].
3. Gwałtowny atak zimy, http://www4.rp.pl/artykul/118113-Gwaltowny-atak-zimy-sparalizowal-Szczecin.html [dostęp: 11.09.2017].
4. Krajowy Plan Zarządzania Kryzysowego, http://rcb.gov.pl/krajowy-plan-zarządzania-kryzysowego/ [dostęp: 16.12.2016].
5. Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) z dnia 2 listopada 2015 r. przyjęty uchwałą Rady Ministrów nr 210/2015, http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf [dostęp: 16.12.2016].
6. Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) z dnia 2 listopada 2015 r. przyjęty uchwałą Rady Ministrów nr 210/2015, http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf [dostęp: 17.08.2017].
7. Operacja antyterrorystyczna na wschodzie Ukrainy, http://www.defence24.pl/75436,operacja-antyterrorystyczna-na-wschodzie-ukrainy [dostęp: 24.01.2016].
8. Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego (2010), RCB, Warszawa, https://rcb.gov.pl/wp-content/uploads/procedura.pdf
9. Risk: Improving government's capability to handle risk and uncertainty; http://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/cabinetoffice/strategy/assets/su%20risk%20summary.pdf
10. Seminarium „Continuity of Government", http://rcb.gov.pl/dwa-dni-o-bezpieczenstwie-panstwa/ [dostęp: 16.12.2016].

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

11. Słownik języka polskiego PWN, https://sjp.pwn.pl/
12. Stracili domy w powodzi, pozwali państwo. Żądają 17 milionów złotych. http://www.tvn24.pl/krakow,50/stracili-domy-w-powodzi-pozwali-panstwo-zadaja-17-milionow-zlotych,407416.html [dostęp: 11.09.2017].
13. Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.) przyjęta uchwałą Rady Ministrów nr 8/2017, https://www.mr.gov.pl/media/36848/SOR_2017_maly_internet_03_2017_aa.pdf [dostęp: 11.09.2017].
14. Zarządzanie ryzykiem i wzmocnienie efektywności służb audytu wewnętrznego w jednostkach sektora finansów publicznych [2007], http://www.mf.gov.pl/c/document_library/get_file?uuid=cfefce1e-fd95-4d0b-b794-207070172a67&groupId=764034 [dostęp: 18.08.2017].
15. Critical Infrastructures: What Makes an Infrastructure Critical? (2003), https://fas.org/irp/crs/RL31556.pdf
16. Diki – internetowy słownik języka angielskiego, https://www.diki.pl/
17. Internetowy słownik języka polskiego PWN, https://sjp.pwn.pl/
18. Internetowy słownik języka angielskiego Cambridge Dictionary https://dictionary.cambridge.org/

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Spis rysunków, schematów i tabel

Rysunek 1. Model przyczynowo-skutkowy klasyfikacji ryzyka 16
Rysunek 2. Matryca ryzyka 65
Rysunek 3. Cykl Deminga 111
Rysunek 4. Źródła sytuacji kryzysowych 155

Spis schematów

Schemat 1. Schemat funkcjonalno-strukturalnego modelu systemu bezpieczeństwa 17
Schemat 2. Fazy zarządzania kryzysowego 33
Schemat 3. Cykl planowania 55
Schemat 4. Działania wynikające ze zidentyfikowania zagrożenia 59
Schemat 5. Algorytm opracowania raportu cząstkowego 60
Schemat 6. System obronny w systemie bezpieczeństwa narodowego 92
Schemat 7. Model funkcjonalno-strukturalny systemu bezpieczeństwa 93
Schemat 8. Model funkcjonalno-strukturalnego systemu bezpieczeństwa z uwzględnieniem ryzyka warunkowego i bezwarunkowego 94
Schemat 9. Zależności pomiędzy sytuacjami kryzysowymi a innymi sytuacjami wynikającymi z występujących zagrożeń 97
Schemat 10. Podział skutków zdarzenia ze względu na podmiot odpowiedzialny .. 115
Schemat 11. Mapa infrastruktury krytycznej i jej poziomów 117
Schemat 12. Zależności zadań zapewniania bezpieczeństwa i ciągłości działania ... 127
Schemat 13. Zarządzanie ryzykiem bezwarunkowym i warunkowym w ramach systemu zarządzania kryzysowego 133
Schemat 14. Przepływ informacji i zasobów w ramach zarządzania sytuacją kryzysową 135
Schemat 15. Etapy osiągania zdolności zarządzania ryzykiem 137
Schemat 16. Powiązanie ryzyka, cech środowiskowych i podatności 149
Schemat 17. Powiązanie ryzyka, cech środowiskowych i podatności wraz ze sprzężeniami zwrotnymi 150
Schemat 18. Wzór matrycy ryzyka sytuacji kryzysowej 153
Schemat 19. Uproszczony model procesu zarządzania w sytuacji kryzysowej po uwzględnieniu wektorów stanu organizacji i otoczenia 160

Spis tabel

Tabela 1. Zależności zachodzące pomiędzy różnymi kategoriami ryzyka w kontekście ich jednolitej kwalifikacji 18
Tabela 2. Klasyfikacja celów badań ze względu na typ badań (kryterium przedmiotowe) 20
Tabela 3. Typy studiów przypadku w zależności od celu badawczego 23
Tabela 4. Ocena prawdopodobieństwa wystąpienia zdarzenia 63

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353

Tabela 5. Ocena skutków zdarzenia ... 63
Tabela 6. Porównanie obszaru objętego UZK i zakresem UMOL ... 67
Tabela 7. Przykład prostej siatki bezpieczeństwa dla fazy reagowania ... 71
Tabela 8. Przykład siatki bezpieczeństwa dla obszaru województwa dla fazy reagowania ... 74
Tabela 9. Przykład siatki bezpieczeństwa dla wszystkich czterech faz zarządzania kryzysowego (fragment) ... 76
Tabela 10. Przykład zadaniowej siatki bezpieczeństwa – cz. 1. Wykaz modułów wraz z ich wykonawcami ... 78
Tabela 11. Przykład zadaniowej siatki bezpieczeństwa – cz. 2. Wykaz wykonawców wraz z realizowanymi modułami dla zagrożenia „Zbiorowe zakłócenie porządku publicznego, w tym zablokowanie przejścia granicznego" ... 81
Tabela 12. Przykład siatki modułowej – cz. 2. Wykaz wykonawców wraz ze zrealizowanymi modułami dla zagrożenia: „Powódź, katastrofalne zatopienie" ... 81
Tabela 13. Porównanie procesów: zarządzania, zarządzania ryzykiem i zarządzania ryzykiem sytuacji kryzysowych ... 96
Tabela 14. Rola zarządzania kryzysowego ... 98
Tabela 15. Komparystyka czystych typów logistyki ... 99
Tabela 16. Porównanie definicji kryzysu w różnych ujęciach ... 101
Tabela 17. Porównanie pojęcia „sytuacja kryzysowa" w różnych ujęciach ... 101
Tabela 18. Porównanie pojęcia „kryzys" w różnych ujęciach ... 102
Tabela 19. Cechy podejścia procesowego i funkcjonalnego w organizacji publicznej 112
Tabela 20. Wykaz sektorów objętych wymogami dyrektywy NIS ... 113
Tabela 21. Różnice w zarządzaniu ryzykiem w skali makro- i mikroekonomicznej .. 115
Tabela 22. Klasyfikacja rodzajów zdarzeń operacyjnych zgodnie z dyrektywą M.... 120
Tabela 23. Wykaz podstawowych procesów realizowanych przez Rządowe Centrum Bezpieczeństwa w ramach zarządzania kryzysowego ... 125
Tabela 24. Kluczowe zasady komunikacji kryzysowej ... 129
Tabela 25. Zarządzanie ryzykiem w ramach systemu zarządzania kryzysowego 134
Tabela 26. Przykładowa tabela kosztów w 1000 PLN przy różnych wariantach reakcji dla wszystkich możliwych wielkości zagrożeń ... 141
Tabela 27. Matryca żalu ... 142
Tabela 28. Zasięg wybranych systemów reagowania ... 159
Tabela 29. Tabela podziału stratygraficznego przypadków do badań ... 173

Plik zabezpieczony watermarkiem jawnym i niejawnym: 14758573A6465353